

# A linearized stabilizer formalism for systems of finite dimension

Niel de Beaudrap\*

Department of Applied Mathematics and Theoretical Physics,  
University of Cambridge, Wilberforce Road, Cambridge, UK

(Dated: 10 September 2012)

The stabilizer formalism is a scheme, generalizing well-known techniques developed by Gottesman [1] in the case of qubits, to efficiently simulate a class of transformations (*stabilizer circuits*, which include the quantum Fourier transform and highly entangling operations) on standard basis states of  $d$ -dimensional qudits. To determine the state of a simulated system, existing treatments involve the computation of cumulative phase factors which involve quadratic dependencies. We present a simple formalism in which Pauli operators are represented using displacement operators in discrete phase space, expressing the evolution of the state via linear transformations modulo  $D \leq 2d$ . We thus obtain a simple proof that simulating stabilizer circuits on  $n$  qudits, involving any constant number of measurement rounds, is complete for the complexity class  $\text{coMod}_d\mathbf{L}$  and may be simulated by  $O(\log(n)^2)$ -depth boolean circuits for any constant  $d \geq 2$ .

Keywords: stabilizer formalism, Weyl operators, Clifford group, symplectic group

## I. INTRODUCTION

Efficiently simulating the evolution of quantum states is a problem of central importance to modern physics. It is generally considered to be a difficult problem: this is formalized by the conjecture that the complexity class  $\mathbf{P}$ , representing decision problems efficiently and deterministically solvable by conventional computers, does not contain  $\mathbf{BQP}$ , the class of decision problems solvable efficiently and with bounded error by using local many-body interactions acting on a standard basis state.

However, some transformations of quantum states are indeed easy to classically simulate. The *stabilizer formalism* is one technique to do so, which may be applied for some evolutions of finite-dimensional systems. Developed by Gottesman [1] to study quantum error correction on qubits, the stabilizer formalism describes how to simulate *stabilizer circuits*: CP maps obtained by composing Clifford group operations (unitary maps which preserve the group generated by Pauli spin operators  $\mathbb{I}$ ,  $\sigma_x$ ,  $\sigma_y$ ,  $\sigma_z$ ), Pauli observable measurements, and Clifford operations controlled directly on measurement outcomes [2]. This serves as a foundation for other efficient simulation techniques [3–5] and for measurement-based quantum computing [6, 7]. It has since been extended in similar ways by Gottesman [8] and by Hostens, Dehaene, and de Moor [9] to systems of qudits of dimension  $d \geq 2$ . This generalization of the stabilizer formalism can be used to simulate circuits involving the quantum Fourier transform (an important element of Shor’s integer factoring algorithm [10]) and certain arithmetic operations on standard basis states (which are closely related to other key operations involved in Shor’s algorithm).

The stabilizer formalism is notable in part for the minimal computational power it requires. Aaronson and Gottesman [11] show that for qubits, simulating stabi-

lizer circuits on computational basis states is feasible for the complexity class  $\oplus\mathbf{L}$ , the subclass of  $\mathbf{P}$  consisting of those problems which are reducible (using logarithmic workspace) to solving systems of linear equations modulo 2 [12]. However, in existing algorithms [11, 13], the exact state of the system is determined by scalar factors which depend quadratically on the exponents of Pauli operators  $\sigma_x^a \sigma_z^b$ ; similar remarks apply to the formalism of Ref. [9] for  $d \geq 2$ . One may ask whether these quadratic dependencies are necessary for the efficient simulation of stabilizer circuits, or if they may be removed to obtain a formalism involving only linear algebra.

This article presents a simple modification to the formalisms of Refs. [9, 11], to simulate stabilizer circuits by solving systems of linear equations modulo  $D \in \{d, 2d\}$ . Using discrete Weyl operators as a matrix basis, rather than the related operators  $\sigma_x^a \sigma_z^b$ , we eliminate quadratic dependencies from simulations to enable Clifford group operations to be simulated entirely linearly. Furthermore, we demonstrate a subgroup of Clifford group which forms a group representation (acting on density operators) of the symplectic group modulo  $D$ , simplifying the connection to symplectic operators described in Ref. [9]. This allows us to obtain direct proofs, for any constant  $d \geq 2$ , that simulating a constant number of measurements in a stabilizer circuit is complete for the complexity class  $\text{coMod}_d\mathbf{L} \subseteq \mathbf{P}$  defined by Buntrock *et al.* [14] generalizing  $\oplus\mathbf{L}$  to arbitrary modulus  $d \geq 2$ . Consequently, all such circuits can be simulated by  $O(\log(n)^2)$ -depth boolean circuits.

Beyond the complexity theoretic results of this article, the formalism that we present here is practically useful for simulations of stabilizer circuits. This (as well as further technical results on Pauli stabilizer groups in the Appendices) should be useful to the study of error correction [15, 16] and measurement-based computation [17] on higher-dimensional systems.

---

\* Contact: niel.debeaudrap@gmail.com

## II. PRELIMINARIES

Throughout,  $d \geq 2$  is a constant. Let  $\mathcal{H}_d = \mathbb{C}^d$  with standard basis vectors  $|q\rangle$  for  $q \in \{0, 1, \dots, d-1\}$ . When little confusion may result, we identify  $q$  with an element of  $\mathbb{Z}_d$  (the ring of integers mod  $d$ ).

Our formalism differs slightly from traditional descriptions of the stabilizer formalism, to achieve as uniform a description as possible while remaining consistent with conventions *e.g.* for the special case  $d = 2$  for qubits. We first address a non-uniformity noted by Refs. [8, 9] between the cases of  $d$  even and  $d$  odd. In analogy to the case  $d = 2$ , we define unitary operators  $X$  and  $Z$  by

$$X|q\rangle = |q+1\rangle \quad \text{and} \quad Z|q\rangle = e^{2\pi i q/d} |q\rangle, \quad (1)$$

using addition mod  $d$ ; then  $X$  and  $Z$  have order  $d$ . We also wish to have an operator  $Y$  which has order  $d$  such that  $XYZ = \tau \mathbb{1}$ , where  $\tau^2 = e^{2\pi i/d}$  (generalizing the equation  $XYZ = i\mathbb{1}$  which holds for qubits). One may show that  $(X^\dagger Z^\dagger)^d = \mathbb{1}$  for  $d$  odd, and  $(X^\dagger Z^\dagger)^d = -\mathbb{1}$  for  $d$  even: the order of  $\tau$  must then depend non-trivially on the parity of  $d$ . We choose  $\tau = e^{i\pi(d^2+1)/d} = (-1)^d e^{i\pi/d}$ , which is consistent with  $\tau = i$  for qubits [18]; then  $(\tau X^\dagger Z^\dagger)^d = \mathbb{1}$  for all  $d$ .

**Definition I:**  $\tau = e^{i\pi(d^2+1)/d}$ , let  $X$  and  $Z$  be defined as in Eq. (1), and  $Y = \tau X^\dagger Z^\dagger$ . The *Pauli group* over  $\mathbb{Z}_d$  is the group  $\mathcal{P}_d = \langle X, Y, Z \rangle = \langle \tau \mathbb{1}, X, Z \rangle$ . The  $n$ -qudit Pauli group  $\mathcal{P}_d^{\otimes n}$  is the group generated by  $n$ -fold tensor products of  $\mathbb{1}$ ,  $X$ ,  $Y$ , and  $Z$ .

To reduce computations for phases in the stabilizer formalism, we describe Pauli operators in terms of translation operators in discrete phase space [19, 20], rather than directly as multiples of  $Z^a X^b$ :

**Definition II:** A *Weyl operator* (on a single qudit) is an operator  $W_{a,b} = \tau^{-ab} Z^a X^b$  for some  $a, b \in \mathbb{Z}$ . On  $n$  qudits, for vectors  $\mathbf{a}, \mathbf{b} \in \mathbb{Z}^n$ , the Weyl operators are

$$\begin{aligned} W_{\mathbf{a},\mathbf{b}} &= W_{a_1,b_1} \otimes \dots \otimes W_{a_n,b_n} \\ &= \tau^{-\mathbf{a} \cdot \mathbf{b}} (Z^{a_1} \otimes \dots \otimes Z^{a_n}) (X^{b_1} \otimes \dots \otimes X^{b_n}), \end{aligned} \quad (2)$$

where  $\mathbf{a} \cdot \mathbf{b}$  is the dot product. For block vectors  $\mathbf{v} = \mathbf{a} \oplus \mathbf{b} \in \mathbb{Z}^{2n}$ , we write  $W_{\mathbf{v}} = W_{\mathbf{a},\mathbf{b}}$ .

The Pauli operators  $\{\mathbb{1}, X, Y, Z\}$  are all Weyl operators (for example,  $Y = W_{-1,-1}$ ); and the set of Weyl operators is invariant under cyclic permutations of  $(X, Y, Z)$  in Definition II. Weyl operators have convenient properties: define the *symplectic inner product* for  $\mathbf{v}, \mathbf{w} \in \mathbb{Z}^{2n}$  by

$$[\mathbf{v}, \mathbf{w}] = \mathbf{v}^\top \sigma_{2n} \mathbf{w}, \quad \text{where} \quad \sigma_{2n} = \begin{bmatrix} 0_n & \mathbb{1}_n \\ -\mathbb{1}_n & 0_n \end{bmatrix}. \quad (3)$$

Note that  $[\mathbf{v}, \mathbf{w}] = -[\mathbf{w}, \mathbf{v}]$ , and  $[\mathbf{v}, \mathbf{v}] = 0$ . The following may be verified by considering actions on the standard basis, using the relation  $X^b Z^a = \tau^{-2ab} Z^a X^b$  for  $a, b \in \mathbb{Z}$ :

**Lemma 1:** For any  $\mathbf{v}, \mathbf{w} \in \mathbb{Z}^{2n}$ , we have  $W_{\mathbf{v}} W_{\mathbf{w}} = \tau^{[\mathbf{v}, \mathbf{w}]} W_{\mathbf{v}+\mathbf{w}}$ . The following properties then also hold:

- (i)  $W_{\mathbf{v}} W_{\mathbf{w}} = \tau^{2[\mathbf{v}, \mathbf{w}]} W_{\mathbf{w}} W_{\mathbf{v}}$ .
- (ii)  $[W_{\mathbf{v}}, W_{\mathbf{w}}] = 0$  if and only if  $[\mathbf{v}, \mathbf{w}] \equiv 0 \pmod{d}$ .
- (iii)  $W_{\mathbf{v}}^t = W_{t\mathbf{v}}$  for  $t \in \mathbb{Z}$ ; in particular,  $W_{\mathbf{v}}^\dagger = W_{-\mathbf{v}}$ .
- (iv) The order of  $W_{\mathbf{v}}$  divides  $d$ .

These properties are a straightforward generalization of observations made by Appleby [19] in his nearly identical formalism for single qudit operators; they are also essentially what allow us to define the formalism of this article. They also suggest a convention of evaluating each vector modulo  $d$ : however, this leads to inconsistencies for  $d$  even. For instance, we have

$$W_{0,1} = Z^0 X^1 = \tau^{2d} Z^d X^1 = -W_{d,1}; \quad (4)$$

as  $W_{d,1}$  is non-zero, we then cannot equate  $W_{0,1}$  to  $W_{d,1}$ . Despite this, it is still possible to use modular arithmetic with the Weyl operators, as outlined in the next lemma:

**Lemma 2:** For all  $\mathbf{v}, \mathbf{w} \in \mathbb{Z}^{2n}$ , we have  $W_{\mathbf{v}} \propto W_{\mathbf{w}}$  if and only if  $\mathbf{w} = \mathbf{v} + d\mathbf{x}$  for some  $\mathbf{x} \in \mathbb{Z}^n$ , in which case

$$W_{\mathbf{w}} = (-1)^{(d+1)[\mathbf{v}, \mathbf{x}]} W_{\mathbf{v}}. \quad (5)$$

In particular,  $W_{\mathbf{v}} = W_{\mathbf{w}}$  if  $\mathbf{v} \equiv \mathbf{w} \pmod{d}$  for  $d$  odd, and if  $\mathbf{v} \equiv \mathbf{w} \pmod{2d}$  for  $d$  even.

This follows from the action of  $W_{\mathbf{v}} W_{\mathbf{w}}^\dagger$  on the standard basis. We may subsume the cases of  $d$  even and  $d$  odd into a single formalism by adopting the following convention:

**Convention:** For  $d \geq 2$ , we define

$$D = \text{the order of } \tau = \begin{cases} d & \text{if } d \text{ is odd,} \\ 2d & \text{if } d \text{ is even;} \end{cases} \quad (6)$$

then the mapping  $\mathbf{v} \mapsto W_{\mathbf{v}}$  is well-defined for  $\mathbf{v} \in \mathbb{Z}_D^{2n}$ , and all associated arithmetic may be performed mod  $D$ .

We frequently describe operations in terms of arithmetic modulo  $D$  — with a notable exception: as standard basis states  $|q\rangle \in \mathcal{H}_d$  involve integers  $q \in \{0, 1, \dots, d-1\}$  by definition, we require expressions involving  $q$  occurring as powers of  $\tau$  to be invariant under replacing  $q$  with  $q \pm d$ .

Consider the Hilbert-Schmidt inner product  $\langle A, B \rangle = \text{Tr}(A^\dagger B)/d^n$ , renormalized to obtain  $\langle \mathbb{1}, \mathbb{1} \rangle = 1$ . From the effect of  $P \in \mathcal{P}_d^{\otimes n}$  on standard basis states, one may easily show  $\text{Tr}(P) \neq 0$  if and only if  $P \propto \mathbb{1}$ . Then for  $P, Q \in \mathcal{P}_d^{\otimes n}$ , either  $P \propto Q$  or  $\langle P, Q \rangle = 0$ , so that:

**Lemma 3:** The following are equivalent for  $\mathbf{v}, \mathbf{w} \in \mathbb{Z}^{2n}$ , for any system of  $n$  qudits of dimension  $d$ :

- (i)  $\langle W_{\mathbf{v}}, W_{\mathbf{w}} \rangle \neq 0$ ;
- (ii)  $\langle W_{\mathbf{v}}, W_{\mathbf{w}} \rangle = \pm 1$ ;
- (iii)  $W_{\mathbf{v}} \propto W_{\mathbf{w}}$ ;
- (iv)  $W_{\mathbf{v}} = \pm W_{\mathbf{w}}$ ;
- (v)  $\mathbf{v} \equiv \mathbf{w} \pmod{d}$ .

Furthermore, when these hold for  $d$  odd,  $W_{\mathbf{v}} = W_{\mathbf{w}}$ .

From this, it is easy to show that a single Weyl operator  $W_{\mathbf{p}}$  can only be generated by a collection of other Weyl operators  $W_{\mathbf{v}_1}, \dots, W_{\mathbf{v}_\ell}$  if  $W_{\mathbf{p}} = \pm W_{\mathbf{v}_j}$  for some operator  $W_{\mathbf{v}_j}$ . By a simple dimension-counting argument, and using the fact that two integers  $0 \leq a, b < d$  are equivalent mod  $d$  if and only if they are equal, we may show:

**Corollary 3a:** The operators  $W_{\mathbf{v}}$  for  $\mathbf{v} \in \{0, \dots, d-1\}^{2n}$  form an orthonormal basis for the linear operators on  $\mathcal{H}_d^{\otimes n}$  with the inner product  $\langle A, B \rangle = \text{Tr}(A^\dagger B)/d^n$ .

Note that the Weyl operators  $W_{\mathbf{v}}$  for  $\mathbf{v} \in \mathbb{Z}_D^{2n}$  are *not* independent for  $D$  even; this is an important technical point in the analysis to follow.

### III. SIMULATING UNITARY STABILIZER CIRCUITS

We now describe a simple formalism, based on Weyl operators, for simulating an important subclass of stabilizer circuits: the class of unitary Clifford circuits, acting on standard basis states, and including at most one final measurement. We refer to these as *unitary stabilizer circuits*.

Note that unitary stabilizer circuits exclude intermediate measurements, or Clifford operations controlled by measurement outcomes. If we are only concerned with the distribution of a single measurement as output, we can still simulate circuits with classically controlled *Pauli* operations conditioned on measurement outcomes, by applying the principle of deferred measurement (as we outline in Section III C). It is also straightforward to apply the techniques of this section to simulate classically controlled Clifford operations, provided the values of the controls do not arise from measurement outcomes.

Unitary stabilizer circuits admit a simple representation in terms of linear transformations modulo  $D$ , simplifying the individual operations used in the existing formalisms for  $d = 2$  and  $d \geq 2$  (in Refs. [1] and [9]). We use this simplified formalism to develop a more general stabilizer formalism which can describe the evolution of states under measurement, for arbitrary qudit dimension  $d$ , in Section IV.

#### A. Stabilizer tableaus for qudits

We begin with a substitute for the so-called binary representation [11, 13] of Pauli operators:

**Definition III:** A *Pauli vector* on  $n$  qudits is a vector  $\bar{\mathbf{v}} \in \mathbb{Z}_D^{2n+1}$  (which we represent as a column vector to enable transformations by left-multiplication), which we decompose into blocks  $\bar{\mathbf{v}} = [\phi \mid v_1 \ v_2 \ \dots \ v_{2n}]^\top$ .

Every Pauli operator  $P$  with order  $\leq d$  is proportional to a Weyl operator by a power of  $\tau^2$ . It suffices to show  $P^d = (\tau^h W_{\mathbf{v}})^d = \mathbb{1}$  if and only if  $\tau^{dh} = 1$ , and solve

modulo  $D$  for  $h$ . Thus we may use Pauli vectors to represent any Pauli operator of order at most  $d$ , using the correspondence

$$\left[ \begin{array}{c} \phi \\ \mathbf{v} \end{array} \right] \mapsto \tau^{-2\phi} W_{\mathbf{v}}. \quad (7)$$

As in the binary case, a *stabilizer group* is an abelian subgroup of Pauli operators which each have  $+1$ -eigenspaces. (Such operators  $P$  may be represented by Pauli vectors: we only have  $P^d \neq \mathbb{1}$  if  $d$  is even and  $P^d = -\mathbb{1}$ , in which case  $P$  has no  $+1$ -eigenspace.) Such a group has a joint  $+1$ -eigenspace: for a set  $\mathcal{S} = \{S_1, \dots, S_\ell\}$  of generators, the projector onto the  $+1$ -eigenspace of  $S \in \mathcal{S}$  is given by

$$\Pi_{\mathcal{S}} = \frac{1}{d} \sum_{j=1}^d S^j; \quad (8)$$

by expanding  $\text{Tr}(\Pi_{S_1} \Pi_{S_2} \dots \Pi_{S_\ell})$  as a sum of traces of Pauli operators, we find that the trace is non-zero.

**Definition IV:** A *stabilizer tableau*  $T_{\mathcal{S}}$  on  $n$  qudits is a matrix over  $\mathbb{Z}_D$  with  $2n+1$  rows, whose columns are Pauli vectors for the generators  $\mathcal{S} = \{S_1, S_2, \dots, S_\ell\}$  of a stabilizer group. The first row  $\phi_{\mathcal{S}}$  of the tableau is called the *phase vector*, and the rest  $W_{\mathcal{S}}$  the *Weyl block* of the tableau. We may present  $T_{\mathcal{S}}$  in terms of  $n \times \ell$  blocks  $X_{\mathcal{S}}$  and  $Z_{\mathcal{S}}$ ,

$$T_{\mathcal{S}} = \left[ \begin{array}{c} \phi_{\mathcal{S}} \\ \hline W_{\mathcal{S}} \end{array} \right] = \left[ \begin{array}{c} \phi_{\mathcal{S}} \\ \hline Z_{\mathcal{S}} \\ \hline X_{\mathcal{S}} \end{array} \right]. \quad (9)$$

This definition corresponds closely to the notation in Refs. [1, 11, 13] for the binary case. The principal distinction between this representation and the binary representation is that the  $Z_{\mathcal{S}}$  and  $X_{\mathcal{S}}$  blocks represent coefficients for Weyl operators, which differ from simple powers of  $Z$  and  $X$  operators on various qudits by scalar factors; and also that the coefficients are defined modulo  $D$ , rather than modulo  $d$ .

The more important distinction is between Weyl operators and simple powers of  $Z$  and  $X$ : while subtle, this difference is significant because of the product formula for Weyl operators in Lemma 1. Consider stabilizer tableaus satisfying a further constraint:

**Definition V:** A stabilizer tableau is *proper* if the columns of its Weyl block  $W_{\mathcal{S}}$  are orthogonal (mod  $D$ ) with respect to the symplectic inner product; *i.e.* if  $W_{\mathcal{S}}^\top \sigma_{2n} W_{\mathcal{S}} \equiv 0 \pmod{D}$ .

As the generators  $S \in \mathcal{S}$  of a stabilizer group commute, the columns of the Weyl block in a corresponding tableau are orthogonal mod  $d$  under the symplectic inner product by Lemma 1; proper tableaus simply satisfy the same

constraints mod  $D$ . Not all stabilizer groups can be represented by proper tableaux (see Section IV A for a simple counterexample); however, every standard basis state  $|q_1 q_2 \cdots q_n\rangle \in \mathcal{H}_d^{\otimes n}$  has a proper tableau of the form

$$\left[ \begin{array}{c|c} q_1 & q_2 & \cdots & q_n \\ \hline & \mathbb{1}_n & & \\ \hline & & & 0_n \end{array} \right]. \quad (10)$$

We may show this by noting that  $|q_j\rangle \in \mathcal{H}_d$  is the state stabilized by  $\tau^{-2q_j} Z$  acting on the  $j^{\text{th}}$  qudit [21]. Furthermore, every stabilizer group has a proper tableau for  $d = 2$  or  $d$  odd; in Appendix A 1, we show how to obtain such a tableau from an “improper” one. We may thus restrict our attention to proper tableaux in many cases.

Given a proper stabilizer tableau, in which we represent Pauli operators in terms of Weyl operators, we may represent recombinations of stabilizer generators using only linear operations on columns, with no further computation of phases:

**Lemma 4:** For two Pauli vectors  $\phi_1 \oplus \mathbf{v}_1$  and  $\phi_2 \oplus \mathbf{v}_2$  drawn from a proper stabilizer tableau, we have

$$[\tau^{-2\phi_1} W_{\mathbf{v}_1}] [\tau^{-2\phi_2} W_{\mathbf{v}_2}] = \tau^{-2(\phi_1 + \phi_2)} W_{\mathbf{v}_1 + \mathbf{v}_2}. \quad (11)$$

This follows directly from Lemma 1. Compare this to multiplication of bare products of  $Z$  and  $X$ , in which  $(Z \otimes Z)(X \otimes X) = (ZX \otimes ZX)$ , but  $(X \otimes Z)(Z \otimes X) = -(ZX \otimes ZX)$ . In the usual binary representation used *e.g.* in Ref. [11], as well as the representation of Ref. [9] for arbitrary  $d \geq 2$ , supplemental phase-factors must be computed depending on which generators are being multiplied; the phases depend quadratically on the exponents of  $X$  and  $Z$  involved in the operator. Our formalism absorbs these quadratic dependencies into the calculus of Weyl operators, so that they do not appear elsewhere in computations involving products of generators. Thus, changes in the generating set of a stabilizer group can be represented using only linear transformations on a proper tableau. As we see in the next section, a representation using Weyl operators allows other transformations of the tableau to be effected linearly as well.

For  $d$  even (*e.g.*, for the case  $d = 2$  corresponding to qubits), stabilizer tableaux are defined modulo  $D = 2d$  rather than mod  $d$ . This difference from Refs. [1, 11, 13] is significant when using Weyl operators to represent Pauli operators, as illustrated in Eq. (4); and varying coefficients of the tableau by  $\pm d$  may not preserve the property of the tableau being proper. In Section IV A, we describe a way in which the Weyl coefficients of a tableau may also be reduced mod  $d$  (though this involves techniques which accommodate improper tableaux). However, the phase vector of a stabilizer tableau may always be evaluated modulo  $d$ , as differences of  $d$  in phase coefficients amount only to a scalar factor of  $\tau^{2d} = +1$  for the operator represented.

## B. The Clifford group on qudits

**Definition VI:** The *Clifford group on  $n$  qudits* is the group of operators  $U \in \mathcal{U}(\mathcal{H}_d^{\otimes n})$  such that  $UPU^\dagger \in \mathcal{P}_d^{\otimes n}$  for any  $P \in \mathcal{P}_d^{\otimes n}$ ; we denote it by  $\mathcal{C}_n(d)$ .

### 1. Linear transformations of stabilizer tableaux

For any  $U \in \mathcal{C}_n(d)$ , the superoperator  $\Phi(M) := U M U^\dagger$  is an automorphism of matrix algebras; we may then reduce the study of the Clifford group to its effect on a generating set  $\{\tau \mathbb{1}, Z_1, Z_2, \dots, X_1, X_2, \dots\}$  of  $\mathcal{P}^{\otimes n}$ . Furthermore,  $\Phi$  maps  $\tau \mathbb{1}$  to itself, and maps each Pauli operator of order  $d$  to another Pauli operator of order  $d$ . Thus we can characterize the effect of an arbitrary Clifford operator on  $n$  qudits by a  $(2n+1) \times (2n+1)$  array over  $\mathbb{Z}_D$  (a “conjugation tableau”),

$$\mathcal{T}_U = \left[ \begin{array}{c|ccc} 1 & h_1 & \cdots & h_{2n} \\ 0 & & & \\ \vdots & & & \\ 0 & & C_U & \end{array} \right], \quad (12)$$

whose columns are vectors representing the images of  $\{\tau^2 \mathbb{1}, W_{\hat{\mathbf{e}}_1}, \dots, W_{\hat{\mathbf{e}}_{2n}}\}$  under  $\Phi$ , in sequence. The effect of conjugating a set  $\mathcal{S}$  of operators given by a tableau as in Eq. (9) by a Clifford unitary  $U$  can be evaluated by matrix multiplication modulo  $\mathbb{Z}_D$ :

$$\left[ \begin{array}{c} \phi_{USU^\dagger} \\ W_{USU^\dagger} \end{array} \right] = \mathcal{T}_U \left[ \begin{array}{c} \phi_{\mathcal{S}} \\ W_{\mathcal{S}} \end{array} \right]. \quad (13)$$

We demonstrate this by identifying a class of Clifford operators whose conjugation tableaux have coefficients  $h_j = 0$  for each  $1 \leq j \leq 2n$ :

**Definition VII:** A *symplectic Clifford operator*  $U \in \mathcal{C}_n(d)$  is one for which  $U W_{\hat{\mathbf{e}}_j} U^\dagger$  is a Weyl operator for each  $1 \leq j \leq 2n$ . We write the set of such operators as  $\sigma \mathcal{C}_n(d)$ .

For  $U \in \mathcal{C}_n(d)$  with a tableau as in Eq. (12), we may decompose  $U = U' W_{\sigma_{2n}\mathbf{h}}$ ; by considering the effect of conjugating each of the Weyl operators  $W_{\hat{\mathbf{e}}_j}$  by  $U W_{\sigma_{2n}\mathbf{h}}^{-1}$ , we may show that  $U' \in \sigma \mathcal{C}_n(d)$ . We then prove Eq. (13) by relating the Weyl blocks  $C_{U'}$  of  $U' \in \sigma \mathcal{C}_n(d)$  to symplectic transformations modulo  $D$ :

**Definition VIII:** A *symplectic transformation* of  $\mathbb{Z}_D^{2n}$  is an operator  $C : \mathbb{Z}_D^{2n} \rightarrow \mathbb{Z}_D^{2n}$  such that  $C^\top \sigma_{2n} C = \sigma_{2n}$ , so that  $C$  preserves the symplectic inner product modulo  $D$ . We denote the group of such operators by  $\text{Sp}_{2n}(\mathbb{Z}_D)$ .

**Theorem 5:** For any  $U \in \sigma \mathcal{C}_n(d)$ , there exists an operator  $C \in \text{Sp}_{2n}(\mathbb{Z}_D)$  such that

$$U W_{\mathbf{v}} U^\dagger = W_{C\mathbf{v}}, \quad \text{for all } \mathbf{v} \in \mathbb{Z}_D^{2n}. \quad (14)$$

In particular,  $\sigma \mathcal{C}_n(d)$  is a group. Similarly, for any  $C \in \text{Sp}_{2n}(\mathbb{Z}_D)$ , there is a  $U \in \sigma \mathcal{C}_n(d)$  for which Eq. (14) holds.

**Proof:** Any  $C \in \text{Sp}_{2n}(\mathbb{Z}_D)$  induces a superoperator  $\Phi$  defined on linear operators acting on  $\mathcal{H}_d^{\otimes n}$ , by extending  $\Phi(W_v) = W_{Cv}$  linearly [22]. As  $C$  is invertible, so is  $\Phi$ ; then  $\Phi \otimes \mathbb{1}$  is a matrix automorphism (where  $\mathbb{1}$  is the identity superoperator on any auxiliary space). In particular,  $\Phi \otimes \mathbb{1}$  maps projectors to projectors; thus it is positive, so that  $\Phi$  itself is completely positive. Finally, as  $\Phi(\mathbb{1}) = \mathbb{1}$  and  $\Phi(W_v)$  has trace zero for  $W_v \neq \mathbb{1}$ , it follows that  $\Phi$  is trace-preserving. Then  $\Phi$  is an invertible CPTP map, so that  $\Phi(M) = U M U^\dagger$  for some  $U \in \sigma\mathcal{C}_n(d)$ .

Conversely, for  $U \in \sigma\mathcal{C}(\mathcal{H}_d^{\otimes n})$ , the map  $M \mapsto U M U^\dagger$  preserves group commutators  $W_v W_w W_v^\dagger W_w^\dagger$  of Weyl operators within the Pauli group. This constrains the Weyl block  $C_U$  of  $\mathcal{T}_U$ : for any  $1 \leq h, j \leq 2n$ , if  $U W_{\hat{e}_h} U^\dagger = W_{v_h}$  and  $U W_{\hat{e}_j} U^\dagger = W_{v_j}$ , we find that  $[v_h, v_j] \equiv [\hat{e}_h, \hat{e}_j] \pmod{d}$ . Thus, the  $2n \times 2n$  array  $C_U$  in fact represents a linear transformation of  $\mathbb{Z}_D^{2n}$  which is symplectic modulo  $d$ . For  $d$  even, we then “lift”  $C_U$  to obtain a matrix  $C'_U \equiv C_U \pmod{d}$  which is symplectic mod  $2d$ . (The procedure to do so is technical, and similar to the procedure for producing proper stabilizer tableaus for  $d$  prime or  $d$  odd: we defer this detail to Appendix A 2.)  $\square$

The above Theorem essentially extends [19, Lemma 2] to the multi-qudit case, albeit expressed here explicitly in terms of symplectic operators  $C$  (rather than invertible operators, which is only equivalent in the case  $n = 1$ ).

**Corollary 5a:** The action of  $U \in \mathcal{C}_n(d)$  by conjugation on Pauli operators may be characterized by Eq. (13).

**Proof:** This is easy to show for Pauli operators, and follows for special Clifford operators from the characterization in terms of  $\text{Sp}_{2n}(\mathbb{Z}_D)$ . Then  $\mathcal{T}_U$  is a product of linear operators arising from these special cases.  $\square$

While Refs. [9, 13] also relate the Clifford group to symplectic operators, we have shown more specifically that  $\sigma\mathcal{C}_n(d) \subset \mathcal{C}_n(d)$  is a group representation of  $\text{Sp}_{2n}(\mathbb{Z}_D)$ . As well, because stabilizer tableaus transform linearly under Clifford operators (with the action on the Weyl block of the tableau being symplectic), we obtain:

**Corollary 5b:** Acting on a proper tableau  $T_S$  by any conjugation tableau  $\mathcal{T}_U$  yields another proper tableau.

## 2. Generators for the symplectic Clifford group

The symplectic Clifford group not only has convenient algebraic properties, but includes the best-known Clifford operators on qudits from the folklore, and analogues of operators from generalizations of the Pauli group to finite fields (*e.g.* Ref. [23]), including the single-qudit operators

$$S = \sum_{q=0}^{d-1} \tau^{q^2} |q\rangle\langle q|, \quad F = \frac{1}{\sqrt{d}} \sum_{p,q=0}^{d-1} \tau^{2pq} |p\rangle\langle q|, \quad (15a)$$

$$M_a = \sum_{q=0}^{d-1} |aq\rangle\langle q|, \quad \text{for } a \in \mathbb{Z}_d^*,$$

where  $\mathbb{Z}_d^*$  stands for the multiplicative group of units modulo  $d$  and where multiplication is performed mod  $d$ ; as well as both of the two-qudit operators

$$\Lambda Z = \sum_{q_1=0}^{d-1} \sum_{q_2=0}^{d-1} \tau^{2q_1 q_2} |q_1\rangle\langle q_1| \otimes |q_2\rangle\langle q_2|; \quad (15b)$$

$$\Lambda X = \sum_{q_1=0}^{d-1} \sum_{q_2=0}^{d-1} |q_1\rangle\langle q_1| \otimes |q_2 + q_1\rangle\langle q_2|. \quad (15c)$$

In the binary case,  $S$  is the  $\pi/4$ -phase gate and  $F$  is the Hadamard gate while  $\Lambda Z$  and  $\Lambda X$  are the controlled- $Z$  and CNOT gates. For  $d \geq 2$  in general,  $F$  is the quantum Fourier transform; and the operators  $M_a$ ,  $X$ , and  $\Lambda X$  can be used to perform any invertible affine transformation modulo  $d$  on the computational basis.

For  $U$  unitary, we write  $A \xrightarrow{U} B$  to denote the relation  $U A U^\dagger = B$  for the sake of brevity. One may easily verify that the above operators  $U$  are symplectic Clifford operators by computing the effect of  $U W_{\hat{e}_j} U^\dagger$  on standard basis states, for  $1 \leq j \leq 2n$ , to verify the following equations:

$$\begin{aligned} Z &\xrightarrow{S} Z, & X &\xrightarrow{S} W_{1,1}, \\ Z &\xrightarrow{F} X^{-1}, & X &\xrightarrow{F} Z, \\ Z &\xrightarrow{M_a} Z^{a^{-1} \pmod{D}}, & X &\xrightarrow{M_a} X^a, \end{aligned} \quad (16a)$$

$$\begin{aligned} Z \otimes \mathbb{1} &\xrightarrow{\Lambda Z} Z \otimes \mathbb{1}, & X \otimes \mathbb{1} &\xrightarrow{\Lambda Z} X \otimes Z, \\ \mathbb{1} \otimes Z &\xrightarrow{\Lambda Z} \mathbb{1} \otimes Z, & \mathbb{1} \otimes X &\xrightarrow{\Lambda Z} Z \otimes X, \end{aligned} \quad (16b)$$

$$\begin{aligned} Z \otimes \mathbb{1} &\xrightarrow{\Lambda X} Z \otimes \mathbb{1}, & X \otimes \mathbb{1} &\xrightarrow{\Lambda X} X \otimes X, \\ \mathbb{1} \otimes Z &\xrightarrow{\Lambda X} Z^\dagger \otimes Z, & \mathbb{1} \otimes X &\xrightarrow{\Lambda X} \mathbb{1} \otimes X, \end{aligned} \quad (16c)$$

all of which are mappings from Weyl operators to Weyl operators [24]. Thus, each such  $U$  may be represented by conjugation tableaus of the form  $\mathbb{1} \oplus C_U$ , for the following symplectic operators  $C_U \in \text{Sp}_{2n}(\mathbb{Z}_D)$ :

$$\begin{aligned} C_S &= \begin{bmatrix} 1 & 1 \\ 0 & 1 \end{bmatrix}, & C_{\Lambda Z} &= \begin{bmatrix} 1 & 0 & 0 & 1 \\ 0 & 1 & 1 & 0 \\ 0 & 0 & 1 & 0 \\ 0 & 0 & 0 & 1 \end{bmatrix}, \\ C_F &= \begin{bmatrix} 0 & 1 \\ -1 & 0 \end{bmatrix}, & & \\ C_{M_a} &= \begin{bmatrix} a^{-1} & 0 \\ 0 & a \end{bmatrix}, & C_{\Lambda X} &= \begin{bmatrix} 1 & -1 & 0 & 0 \\ 0 & 1 & 0 & 0 \\ 0 & 0 & 1 & 0 \\ 0 & 0 & 1 & 1 \end{bmatrix}. \end{aligned} \quad (17)$$

Not only do these operators represent a collection of well-known operators which happen to belong to the symplectic Clifford group, they also characterize it:

**Lemma 6:** The operators  $S$ ,  $F$ ,  $\Lambda Z$  (or  $\Lambda X$ ), and  $M_a$  for  $a$  ranging over the multiplicative units of  $\mathbb{Z}_D$ , generate  $\sigma\mathcal{C}_n(d)$  up to global phase factors.

**Proof:** We show this result by showing that the operators  $C_{\Lambda X}$ ,  $C_S$ ,  $C_F$ , and  $C_{M_a}$ , together with direct sums with  $\mathbb{1}_2$  corresponding to tensor products with the identity operator on qudits [25], generate the group  $\text{Sp}_{2n}(\mathbb{Z}_D)$ . This result is technical, and we prove it by reduction to a similar result shown in Ref. [9, Sec. IV] (see note [26]). Using Eq. (16), one may show that  $\Lambda X = (\mathbb{1} \otimes F^\dagger) \Lambda Z (\mathbb{1} \otimes F)$ , so that selecting either  $\Lambda X$  or  $\Lambda Z$  as a generator is equivalent. We may also describe  $\Lambda X_{2,1}$ , a reversed version of  $\Lambda X_{1,2} := \Lambda X$  (*i.e.* where  $\Lambda X_{2,1}$  has the second qudit the control, and the first qudit the target), by  $\Lambda X_{2,1} = (F^\dagger \otimes \mathbb{1}) \Lambda Z (F \otimes \mathbb{1})$ . It is easy to show that for  $g \in \mathbb{Z}$ , the operator  $\Lambda X_{2,1}^{-g}$  has a conjugation tableau of the form  $1 \oplus C_\chi^{-g}$ , where

$$C_\chi^{-g} = \begin{bmatrix} 1 & 0 & 0 & 0 \\ g & 1 & 0 & 0 \\ 0 & 0 & 1 & -g \\ 0 & 0 & 0 & 1 \end{bmatrix}. \quad (18)$$

We can also generate  $\text{SWAP}_{1,2}$  gates on pairs of qudits, which interchange  $Z_1$  and  $Z_2$ , and similarly  $X_1$  and  $X_2$ : routine calculation will show that we may decompose  $\text{SWAP}_{1,2} = (F^2 \otimes \mathbb{1}) \Lambda X_{1,2} \Lambda X_{2,1}^\dagger \Lambda X_{1,2}$ . By construction, it has a conjugation map of the form  $1 \oplus C_\varsigma$  for

$$C_\varsigma = \begin{bmatrix} 0 & 1 & 0 & 0 \\ 1 & 0 & 0 & 0 \\ 0 & 0 & 0 & 1 \\ 0 & 0 & 1 & 0 \end{bmatrix}. \quad (19)$$

Finally, the conjugation map of the operator  $FS^{-g}F^\dagger$  for  $g \in \mathbb{Z}$  is the operator  $1 \oplus C_F C_S^{-g} C_F^{-1}$ , where one may compute

$$C_F C_S^{-g} C_F^{-1} = \begin{bmatrix} 1 & 0 \\ g & 1 \end{bmatrix}. \quad (20)$$

The three operators of Eqs. (18) – (20), together with the operators  $C_F$  and  $C_{M_r}$ , are precisely those used in Ref. [9, Sec. IV] to decompose arbitrary symplectic operators modulo  $D$ .

Thus an arbitrary conjugation tableau for an operator  $U \in \sigma\mathcal{C}_n(d)$  may be generated by those of the operators  $S$ ,  $F$ ,  $\Lambda Z$ , and  $M_a$ ; as  $U$  is characterized up to scalar factors by its conjugation tableau, the Lemma follows.  $\square$

### C. Deferring measurements in stabilizer circuits

For qudits of dimension  $d \geq 2$ , most Pauli operators are non-Hermitian. For a Pauli operator  $P$  of order at most  $d$ , we use the phrase “measurement of  $P$ ” as shorthand, to refer to measurement of any Hermitian operator  $H$  with a spectral diameter less than  $2\pi$ , such that  $P = \exp(iH)$ . This amounts to collapsing the state of the system onto one of the eigenspaces of  $P$  via projective

measurement, obtaining a record  $h \in \mathbb{Z}_d$  of the eigenvalue  $\tau^{2h}$  associated to that eigenspace.

For reasons that will become apparent in Section IV, describing the evolution of a state under a non-destructive measurement is more complicated for  $d \geq 2$  arbitrary than for  $d$  prime. This is an obstacle to simulating circuits which involve both multiple measurements, and unitary operations which are conditioned on measurement outcomes. We may overcome this by applying the principle of deferred measurement, postponing all measurements to the end without affecting the measurement statistics (or final residual quantum states). This will allow us to efficiently simulate stabilizer circuits with classically-controlled Pauli operations (but not classically-controlled Clifford operations in general) using the techniques described thus far, so that we may consider the statistics of any single measurement unconditionally from any measurement which precedes it. We may perform such simulations as follows.

#### 1. Reduction to $Z_r$ measurements

As in the binary case [11], there is no loss of generality in restricting from general Pauli measurements to “non-destructive”  $Z$  measurements (*i.e.* in which the measured qudit has a defined post-measurement state). For a  $W_{\mathbf{p}} \in \mathcal{P}_d^{\otimes n}$  measurement, this may be done in a straightforward way by constructing a  $\Lambda W_{\mathbf{p}}$  (“controlled  $W_{\mathbf{p}}$ ”) operator, which on standard basis states  $|c\rangle \in \mathcal{H}_d$  and  $|t\rangle \in \mathcal{H}_d^{\otimes n}$  would perform the operation

$$\Lambda W_{\mathbf{p}} |c\rangle |t\rangle = |c\rangle \otimes W_{\mathbf{p}}^c |t\rangle. \quad (21)$$

We may construct  $W_{\mathbf{p}} \in \mathcal{P}_d$  on a single qudit straightforwardly out of  $\Lambda Z$  and  $\Lambda X$  gates. To illustrate this, consider the decomposition of  $W_{\mathbf{p}}$  into  $Z$ ,  $X$ , and a “global phase” gate, as illustrated in Fig. 1.

$$\boxed{W_{p_1, p_2}} \equiv \boxed{X^{p_2}} \boxed{Z^{p_1}} \boxed{\tau^{-p_1 p_2} \mathbb{1}}$$

FIG. 1. A notional circuit for a  $W_{\mathbf{p}}$  gate on one qudit.

To obtain a coherently controlled version, given that  $W_{\mathbf{p}}^c = W_{c\mathbf{p}} = \tau^{-c^2 p_1 p_2} Z^{c p_1} X^{c p_2}$ , we replace the  $Z$  and  $X$  gates with  $\Lambda Z$  and  $\Lambda X$  gates on a common control qudit, and act on the control with  $S^{-p_1 p_2}$  satisfying  $S^{-p_1 p_2} |c\rangle = \tau^{-c^2 p_1 p_2} |c\rangle$ . Then we may decompose  $\Lambda W_{\mathbf{p}} = (S^{-p_1 p_2} \otimes \mathbb{1}) \Lambda Z^{p_1} \Lambda X^{p_2}$  for single-qudit Weyl operators illustrated in Fig. 2. For a multi-qudit Weyl operator  $W_{\mathbf{p}} = W_{p_1, p_{n+1}} \otimes W_{p_2, p_{n+2}} \otimes \cdots \otimes W_{p_n, p_{2n}}$  where  $n > 1$ , we decompose  $\Lambda W_{\mathbf{p}}$  into operators  $\Lambda W_{p_j, p_{n+j}}$  acting with a common control and distinct targets. Using the Fourier transform  $F$  on the control qudit, we may apply standard techniques for eigenvalue estimation [27] to perform a  $W_{\mathbf{p}}$  measurement using a  $Z$  observable measurement on the control, as illustrated in Figure 3.

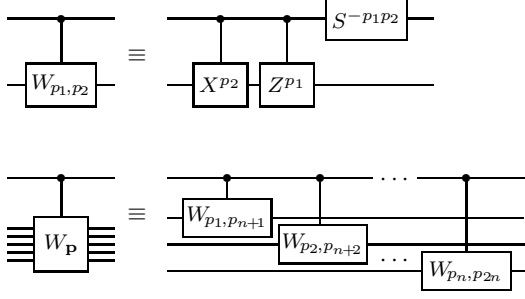


FIG. 2. Circuits for  $\Lambda W_{\mathbf{p}}$  gates, for  $W_{\mathbf{p}} \in \mathcal{P}_d$  and  $W_{\mathbf{p}} \in \mathcal{P}_d^{\otimes n}$ .

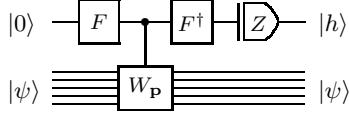


FIG. 3. Circuit to perform a measurement of an  $n$ -qudit Weyl operator  $W_{\mathbf{p}}$ , using a  $Z$  measurement on the top qudit to obtain the result. (This is illustrated here for measurement of a  $\tau^{2h}$ -eigenstate of  $W_{\mathbf{p}}$ , where the outcome will be  $h$ .)

Measurement of a Pauli operator  $P = \tau^{2\delta} W_{\mathbf{p}}$  may be performed similarly by replacing  $\Lambda W_{\mathbf{p}}$  with a controlled- $P$  gate,  $\Lambda P = (Z^\delta \otimes \mathbb{1}^{\otimes n}) \Lambda W_{\mathbf{p}}$ . These substitutions may be easily performed at the time of simulation.

## 2. Qudit states as measurement records

While it is common to conceive of single-qudit measurements as being destructive, replacing the measured qudit with a classical record, we consider the qudit  $r$  on which we perform the  $Z$  observable measurement to be a persistent quantum system whose state is the measurement record. To retain consistency with the notion of a classical measurement record, we may impose constraints of the following sort:

- We may require that no operators act on the qudit  $r$  (after the measurement) aside from those which commute with  $Z_r$ . For instance, it may act as the control of a product of  $\Lambda X$  or  $\Lambda Z$  operators, instead of acting as a classical control for Pauli operators on the same target qudits. In this case, the state of the qudit  $r$  remains an unchanging record of the measurement outcome.
- We may instead allow measured qudits  $r$  to be subject to Pauli operators themselves, with classical control limited only to qudits  $s$  which are also measurement records or input parameters. Such transformations of the measured qubits are limited to invertible transformations of the standard basis over  $\mathbb{Z}_d$ , and may be simulated in the stabilizer formalism by representing them as Clifford group operators.

Using these restrictions, we may commute  $Z$  measurements on measurement registers past any Pauli operators which are conditioned on the outcome of that measurement. If a measurement record acts only as a classical control for Pauli operations, both the distribution of outcomes for  $r$  and the final state of any system depending on  $r$  is unaffected by commuting the  $Z_r$  measurement past the controlled operation. More generally, while a controlled transformation depending on a measurement record  $s$  will transform  $Z_r$  non-trivially, the *group* of observables  $\langle Z_m, \dots, Z_r, Z_s \rangle$  on the measurement records is preserved; so measuring  $Z_m, \dots, Z_s$  after the transformations will yield the same distribution of outcomes, as measuring  $Z_m, \dots, Z_s$  first and then transforming the outcomes. With either approach, one may simulate all classically controlled operations  $P \in \mathcal{P}_d^{\otimes n}$  which depend on measurement outcomes using the corresponding *coherently* controlled operators  $\Lambda P$ . The distribution of any single measurement outcome may then be simulated using the techniques described thus far.

## 3. Remarks on classically controlled Clifford operations

Deferring measurements cannot be done for measurement records which control Clifford operations while remaining in the stabilizer formalism, using the techniques described above, except for controlled-Pauli operations. Even in the simplest case, acting on states in which the control is in a standard basis state, such a simulation would involve transforming some columns of the tableau (*i.e.* representing Pauli operators supported on the target qudits of the operation) with different linear transformations depending on the values of other columns (which represent Pauli operators supported on the control qudit of the operation). Such a transformation is at best multilinear, but not linear. Furthermore, this transformation would be ill-defined for any column in which the control qudit is acted on by an operator with a non-zero  $X$  component. For instance, the coherently controlled operator  $\Lambda S$  obtained by deferring the measurement on the control acts on the operator  $X \otimes \mathbb{1}$  as follows:

$$\begin{aligned} \Lambda S(X \otimes \mathbb{1}) \Lambda S^\dagger |c\rangle |t\rangle &= \begin{cases} (X \otimes S) |c\rangle |t\rangle, & \text{if } c \in \{0, \dots, d-2\}, \\ (X \otimes S^{1-d}) |c\rangle |t\rangle, & \text{if } c = d-1. \end{cases} \end{aligned} \quad (22)$$

Thus,  $\Lambda S$  fails to map  $X \otimes \mathbb{1}$  to another Pauli operator via conjugation, and isn't represented by a transformation of stabilizer tableaus. (Indeed, as it fails to preserve the Clifford group, such an operator  $\Lambda S$  is not itself a Clifford operator; supplementing the Clifford group with any single non-Clifford unitary generates a set of operators approximately universal for quantum computation for  $d = 2$  [28] as well as any other prime dimension [29, Appendix D], so that classical algorithms to simulate TOFFOLI gates together with Clifford operations are impossible unless  $\text{BPP} = \text{BQP}$ .) To simulate a Clifford

operation controlled by measurement outcomes, we must therefore explicitly compute (the probability distribution of) the measurement outcome, and use this outcome to determine mid-simulation which linear transformation to apply to the target qudits.

For any fixed measurement outcome, or for a classical control value provided as input (or generated according to a fixed probability distribution), simulating a classically controlled Clifford operation is no more difficult than a fixed Clifford operation; the only obstacle in this case is simulating the evolution of the state caused by the measurement itself, which we treat in Section IV.

#### D. Computing the distribution of a single terminal measurement

Describing the evolution of a state under measurement proves to be more technically complicated in the case of composite dimensions  $d \geq 2$ , as we shall see in Section IV. However, determining the distribution of outcomes for a single measurement, on a state which can be represented by a proper stabilizer tableau, can be treated using the techniques described thus far. We now summarize how to determine the distribution over possible outcomes, deferring the account of how states transform under measurement for Section IV, and proofs of certain details to Appendix B.

Consider a proper stabilizer tableau  $T_S$  which represents a group  $G_S$  stabilizing a unique state. To simulate measurement with respect to a Pauli operator  $P$ , consider some Weyl operator  $W_P \propto P$ . While  $W_P$  may not commute with all elements of  $G_S$ , there may be a non-trivial power of  $W_P$  which does. The smallest positive power  $s \geq 1$  such that  $W_P^s$  does commute with all of  $G_S$  constrains the distribution of possible measurement outcomes for  $P$ . By Lemma 1,  $s$  is the smallest positive integer such that  $[s\mathbf{p}, \mathbf{v}_k] \equiv 0 \pmod{d}$ , where  $\varphi_k \oplus \mathbf{v}_k$  is the  $k^{\text{th}}$  column of  $T_S$ . That is,  $s$  is the smallest positive integer such that

$$s(0 \oplus \mathbf{p})^\top (0 \oplus \sigma_{2n}) T_S \equiv \mathbf{0}^\top \pmod{d}. \quad (23)$$

From the minimality of  $s$ , it follows that  $s$  will be a factor of  $d$ , with  $s = 1$  in the case that  $W_P$  commutes with  $G_S$ . Specifically, let  $\phi = (0 \oplus \mathbf{p})^\top (0 \oplus \sigma_{2n}) T_S$ , and consider the greatest common factor  $\eta$  of the coefficients of  $\phi$  together with  $d$ : then  $s = d/\eta$ . As  $W_P^s$  commutes with all of the generators of  $G_S$ , and as  $G_S$  stabilizes a unique state, we may show (Lemma 12) that  $W_P^s$  is proportional to an element of  $G_S$ . Then the pre-measurement state is an eigenstate of  $W_P^s$ , whose eigenvalue constrains the possible measurement outcomes. If it is a  $\tau^{2t}$ -eigenstate, then  $\tau^{-2t} W_{s\mathbf{p}}$  stabilizes the state, in which case there is a vector  $t' \oplus s\mathbf{p}'$  in the column-span of  $T_S$  such that  $\tau^{-2t} W_{s\mathbf{p}} = \tau^{-2t'} W_{s\mathbf{p}'}$ . In order for this equality to hold, we require that  $s\mathbf{p}' - s\mathbf{p} \equiv 0 \pmod{d}$ , and that  $2t' - 2t \equiv [s\mathbf{p}', s\mathbf{p}] \pmod{D}$  as well.

- For  $d$  odd, these two conditions imply that  $t' - t \equiv 0 \pmod{d}$ , so that we simply need to determine for which value of  $t \in \mathbb{Z}_D$  that  $t \oplus s\mathbf{p}$  is in the column span of  $T_S$ .
- For  $d$  even, the vector  $t' \oplus s\mathbf{p}'$  may differ from  $t \oplus s\mathbf{p}$ . In particular, we may have  $t'$  and  $t$  may differ by  $\frac{d}{2}$  modulo  $d$ ; and the vector  $d\mathbf{x} = s\mathbf{p}' - s\mathbf{p}$  corresponds to some representation of the identity operator  $\mathbb{1} = W_{d\mathbf{x}}$  which accounts for the difference in the phase coefficients, by the formula

$$\begin{aligned} \tau^{-2t'} W_{s\mathbf{p}'} &= \tau^{-2t + [d\mathbf{x}, s\mathbf{p}]} W_{s\mathbf{p} + d\mathbf{x}} \\ &= \tau^{-2t} W_{s\mathbf{p}} W_{d\mathbf{x}}, \end{aligned} \quad (24)$$

by Lemma 2. We may attempt to account for the contribution of  $W_{d\mathbf{x}}$  to the phases by introducing auxiliary columns of the form  $\mathbf{u}_j := \frac{d}{2} [\hat{\mathbf{e}}_j, s\mathbf{p}] \oplus d\hat{\mathbf{e}}_j$  to the tableau  $T_S$ : adding  $\mathbf{u}_j$  to  $(t \oplus \mathbf{p})$  yields another Pauli vector representing the same operator. We may also introduce a column  $\mathbf{u}_0 = (d \oplus \mathbf{0})$ , also representing the identity operator, to account for differences of  $\pm d$  in the phase coefficient which are insignificant. Thus, it suffices to determine for which value of  $t \in \mathbb{Z}_D$  that  $(t \oplus s\mathbf{p})$  is in the column span of  $[\mathbf{u}_0 \ \mathbf{u}_1 \ \cdots \ \mathbf{u}_{2n} \mid T_S]$ .

In either case, it suffices to adjoin the vector  $-(0 \oplus s\mathbf{p})$  to the tableau (together with the vectors  $\mathbf{u}_j$  in the case of  $d$  even), and perform column-reductions to clear the Weyl tableau. The resulting matrix will contain a vector  $(t \oplus \mathbf{0})$ , which implies that  $(t \oplus s\mathbf{p})$  is the column span of the original matrix and that the pre-measurement state is a  $\tau^{2t}$ -eigenstate of  $W_{s\mathbf{p}}$ .

The constraint that this imposes on the outcomes of a  $W_P$  measurement are as follows. As  $(\tau^{-2t} W_{s\mathbf{p}})^s$  is proportional to  $\mathbb{1}$  and has  $+1$ -eigenstates, we have  $2t\eta \equiv 0 \pmod{D}$ , from which it follows that  $t$  is a multiple of  $s$ . The post-measurement state is a  $\tau^{2u}$ -eigenstate of  $W_P$  by definition for some  $u \in \mathbb{Z}_d$ , and in particular must be a  $\tau^{2t}$ -eigenstate of  $W_P^s$  as noted above; thus  $2t \equiv 2su \pmod{D}$ , or equivalently  $u \equiv t/s \pmod{\eta}$ . We show in Appendix B 3 that the outcomes are in fact uniformly distributed over all  $u \in \mathbb{Z}_d$  satisfying this constraint. This characterizes the probability distribution over the outcome  $\tau$  of the measurement of  $W_P$ . For  $P = \tau^{-2\delta} W_P$ , the distribution of outcomes for a  $P$  measurement are uniform over the solutions  $h \in \mathbb{Z}_d$  to the congruence

$$h \equiv u + \delta \equiv t\eta/d + \delta \pmod{\eta}, \quad (25)$$

where again  $\eta = \gcd(d, \phi_1, \phi_2, \dots)$ . In particular, the results are uniformly distributed over some coset  $\kappa + \eta\mathbb{Z}_d$ , where we may take  $\kappa = t\eta/d + \delta$ .

Note that the above analysis accommodates the possibility of a deterministic outcome. If  $P$  commutes with  $G_S$ , then  $\eta = d$ , in which case Eq. (25) has a unique solution mod  $d$ : the outcomes are “uniformly” distributed over a singleton set (*i.e.* follow a delta-distribution). This



analysis also generalizes the familiar scenario of a random measurement outcome for  $d$  prime: in that special case, we have  $\eta = 1$  if the measurement observable  $P$  does not commute with all elements of  $\mathcal{S}$ . In the case  $\eta = 1$ , Eq. (25) trivializes and imposes no constraints on  $h \in \mathbb{Z}_d$ , and so is uniformly distributed over  $\mathbb{Z}_d$ .

### E. Summary for simulating unitary stabilizer circuits

We have shown that using Weyl operators to describe stabilizer tableaux allows us to describe a simple, linear formalism for representing the action of Clifford circuits on standard basis states, and determining the measurement outcomes for single measurements. These results follow from the special algebraic properties of Weyl operators as described in Lemma 1, and the fact that standard basis states may be represented by proper tableaux (as defined in Section III A). Demonstrating a subgroup  $\sigma\mathcal{C}_n(d) \subset \mathcal{C}_n(d)$  which is a representation of  $\text{Sp}_{2n}(\mathbb{Z}_D)$  is an additional dividend of this formalism.

The remainder of the article is devoted to extending this formalism to explicitly describe the evolution of stabilizer states under measurements, which involves providing a linear analysis of those states which lack “proper” stabilizer tableaux as described in Section III A.

## IV. IMPROPER TABLEAUS AND EVOLUTION UNDER MEASUREMENTS

As we note on page 4 (and show below), there do not always exist proper stabilizer tableaux for a stabilizer state in the case of even  $d > 2$ . Furthermore, measurements may transform a state stabilized by a group with a proper tableau, to one stabilized by a group without any proper tableau. This presents an obstacle for a uniform treatment of stabilizer circuits in the manner we have described so far, and are unavoidable when simulating the distributions of outcomes of circuits involving multiple measurements for even  $d > 2$ . We must therefore extend the formalism described thus far to describe a linear formalism to simulate arbitrary stabilizer circuits, and simulate outcomes of multiple measurements.

### A. Extension to accommodate states having no proper tableaux

For even dimensions  $d > 2$ , there are stabilizer states whose stabilizer groups cannot be represented by a proper stabilizer tableau. The simplest example is the single-qudit state  $\frac{1}{\sqrt{2}}(|0\rangle + |2\rangle)$  for  $d = 4$ , which is stabilized by the set  $\mathcal{S} = \{Z^2, X^2\}$ . This set of generators has four possible stabilizer tableaux (up to column swaps

and inconsequential changes in the phase block):

$$\begin{bmatrix} * & * \\ 2 & 0 \\ 0 & 2 \end{bmatrix}, \quad \begin{bmatrix} * & * \\ 2 & 0 \\ 0 & 6 \end{bmatrix}, \quad \begin{bmatrix} * & * \\ 6 & 0 \\ 0 & 2 \end{bmatrix}, \quad \begin{bmatrix} * & * \\ 6 & 0 \\ 0 & 6 \end{bmatrix}; \quad (26)$$

where each  $*$  may independently be either 0 or 4 (representing a global phase of  $+1$ ). The reader may verify that none of these are proper, as the columns of the Weyl blocks are not orthogonal under the symplectic product modulo  $D = 8$ . Thus, there do not exist any proper stabilizer tableaux for  $\mathcal{S}$ ; by linearity, there are no proper tableaux for any other set of operators generating the same group either.

As the Pauli vectors of commuting operators are always orthogonal mod  $d$  under the symplectic inner product, such obstacles do not arise for  $d$  odd. In the case of  $d = 2$ , while “improper” tableaux do exist, every stabilizer state has a proper tableau, which may be obtained from an improper one by the techniques of Appendix A 1. However, to describe a formalism which functions for arbitrary  $d$ , it is necessary to incorporate corrections to the phases as in the standard “binary” formalism, in order to describe different generating sets of the stabilizer group. We show that these corrections may be subsumed in a more general linear formalism, as follows.

#### 1. Extended stabilizer tableaux

Consider a set of commuting Pauli vectors  $\mathbf{p}_1, \dots, \mathbf{p}_\ell$ , where each vector  $\mathbf{p}_j = [\phi_j | \mathbf{v}_j]^\top$  represents a Pauli operator  $P_j = \tau^{-2\phi_j} W_{\mathbf{v}_j}$ . By Lemma 1, we have  $W_{\mathbf{u}} W_{\mathbf{v}} = \tau^{[\mathbf{u}, \mathbf{v}]} W_{\mathbf{u} + \mathbf{v}}$ , where  $[\mathbf{u}, \mathbf{v}] \equiv [\mathbf{v}, \mathbf{u}]$  as  $P_h$  and  $P_j$  commute. It follows that  $[\mathbf{u}, \mathbf{v}] \in \{0, d\}$  modulo  $D$ . These represent corrections to the phase coefficients of Pauli vectors by multiples of  $\frac{d}{2}$  (which would always be 0 in the case of  $d$  odd). When computing products of the Pauli operators  $P_j$ , we may avoid computing the quadratic dependency arising from the symplectic inner products  $[\mathbf{v}_h, \mathbf{v}_j]$  by storing an array  $\Xi \in \{0, \frac{d}{2}, d, \frac{3d}{2}\}^{\ell \times \ell}$  such that  $\Xi_{h,j} \equiv \frac{1}{2} [\mathbf{v}_h, \mathbf{v}_j] \pmod{D}$ . We may do this using an expanded table of coefficients, of the form

$$\bar{T}_{\mathcal{S}} = \begin{bmatrix} \phi_1 & \cdots & \phi_\ell \\ \mathbf{v}_1 & \cdots & \mathbf{v}_\ell \\ \Xi \end{bmatrix}. \quad (27)$$

We call such an array an *extended stabilizer tableau*, and refer to  $\Xi$  as the *phase correction block* of the tableau; the tableau  $\bar{T}_{\mathcal{S}}$  is proper if  $\Xi \equiv 0 \pmod{D}$ . In the case of  $d$  odd, this in fact holds by necessity.

Products and recombinations of generators may be represented by linear *superoperators* on such extended tableaux, differing only slightly from left- and right-matrix-multiplications on  $\bar{T}_{\mathcal{S}}$ . For each  $1 \leq j \leq \ell$ , let

$\bar{\mathbf{p}}_j = \mathbf{p}_j \oplus \Xi \hat{\mathbf{e}}_j$  be the column of  $\bar{T}_S$  extending  $\mathbf{p}_j$ . Consider a product of Pauli operators:

$$\tilde{P} = P_h P_j = \tau^{-2(\phi_h + \phi_j + \Xi_{h,j})} W_{\mathbf{v}_h + \mathbf{v}_j}. \quad (28)$$

Let  $\tilde{\varphi} = \phi_h + \phi_j + \Xi_{h,j}$  for the sake of brevity. When taking products of  $\tilde{P}$  with other operators  $P_k$ , the quadratic dependency involved in the phases depends only on the Weyl operator  $W_{\mathbf{v}_h + \mathbf{v}_j}$ , to which  $\tilde{P}$  is proportional. Therefore we have

$$\begin{aligned} \tilde{P} P_k &= \tau^{-2(\tilde{\varphi} + \phi_k + [\mathbf{v}_h + \mathbf{v}_j, \mathbf{v}_k]/2)} W_{(\mathbf{v}_h + \mathbf{v}_j) + \mathbf{v}_k} \\ &= \tau^{-2(\tilde{\varphi} + \phi_k + [\Xi_{h,k} + \Xi_{j,k}])} W_{(\mathbf{v}_h + \mathbf{v}_j) + \mathbf{v}_k}; \end{aligned} \quad (29)$$

where the phase correction  $[\Xi_{h,k} + \Xi_{j,k}]$  is a sum of the phase corrections arising from  $P_h$  and  $P_j$ . Then, we may represent operator  $\tilde{P}$  by an extended column vector of the form

$$\tilde{\mathbf{p}} = \begin{bmatrix} \phi_h + \phi_j + \Xi_{h,j} \\ \mathbf{v}_h + \mathbf{v}_j \\ \Xi \hat{\mathbf{e}}_h + \Xi \hat{\mathbf{e}}_j \end{bmatrix} = \bar{\mathbf{p}}_h + \bar{\mathbf{p}}_j + \begin{bmatrix} \Xi_{h,j} \\ \mathbf{0} \\ \mathbf{0} \end{bmatrix}. \quad (30)$$

Thus to obtain the extended tableau  $\bar{T}_S$  in which the generator  $P_j$  is replaced with  $\tilde{P} = P_h P_j$ , it suffices to add the  $h^{\text{th}}$  column into the  $j^{\text{th}}$  column, subtract the  $h^{\text{th}}$  row (of the phase-correction block) from the  $j^{\text{th}}$  row to maintain the antisymmetry of that submatrix, and finally add the corrective term  $\Xi_{h,j}$  into the phase coefficient. That is, we compute

$$\bar{T}_S = \Psi_{h,j} \left( E_{2n+1+h, 2n+1+j}^{-1} \bar{T}_S E_{h,j} \right), \quad (31a)$$

where  $E_{a,b} = \mathbb{1} + \hat{\mathbf{e}}_a \hat{\mathbf{e}}_b^\top$  is the usual elementary matrix for adding row  $a$  into row  $b$ , and where

$$\Psi_{h,j}(M) = M + [\hat{\mathbf{e}}_1 \hat{\mathbf{e}}_{2n+1+h}^\top] M [\hat{\mathbf{e}}_j \hat{\mathbf{e}}_j^\top] \quad (31b)$$

is a superoperator which adds the appropriate phase correction (stored in the  $j^{\text{th}}$  column) for the operators represented by columns  $h$  and  $j$ , to the phase coefficient of column  $j$ .

## 2. Reducing the extended tableau modulo $d$

In the case that  $d$  is odd, we have  $D = d$ , and the entire tableau remains reduced modulo  $d$  at all times. However, if  $d$  is even, coefficients  $c \in \{d, d+1, \dots, 2d-1\}$  may arise. Though these coefficients never present any actual difficulties in representing stabilizer states, it is still possible to reduce such coefficients modulo  $d$  by performing phase corrections if this is desired. As an extended tableau is under no restrictions to remain proper, we may more freely choose which Pauli vectors we use to represent a given Pauli operator generating a stabilizer group, so long as we maintain the correct phase correction information.

For a single Pauli vector, we may reduce the Weyl block modulo  $d$  by considering different representations of the identity operator  $\mathbb{1}$  by Pauli vectors, such as

$$\begin{aligned} \mathbb{1} &= W_{d\hat{\mathbf{e}}_1} = Z_1^d, & \dots, & \quad \mathbb{1} = W_{d\hat{\mathbf{e}}_n} = Z_n^d, \\ \mathbb{1} &= W_{d\hat{\mathbf{e}}_{n+1}} = X_1^d, & \dots, & \quad \mathbb{1} = W_{d\hat{\mathbf{e}}_{2n}} = X_n^d. \end{aligned} \quad (32)$$

This corresponds to Pauli vector representations of the form  $0 \oplus d\hat{\mathbf{e}}_h$  for  $1 \leq h \leq 2n$ . The phase correction required to combine such a vector with an arbitrary Pauli vector  $\varphi \oplus \mathbf{v}$  is given by

$$\tilde{\xi}_h = \frac{1}{2} [d\hat{\mathbf{e}}_h, \mathbf{v}] \equiv \begin{cases} \frac{d}{2} v_{h+n}, & \text{if } 1 \leq h \leq n; \\ -\frac{d}{2} v_{h-n}, & \text{if } n < h \leq 2n, \end{cases} \quad (33)$$

modulo  $D$ . Because  $-\frac{d}{2} \equiv d + \frac{d}{2} \pmod{D}$  for  $d$  even, and differences of  $d$  have no effect in the phase columns, the phase corrections of  $-\frac{d}{2}$  may be replaced by phase corrections of  $+\frac{d}{2}$ , or vice versa. Reduction modulo  $d$  of the Weyl coefficients of Pauli vectors can then be performed with the transformations

$$\begin{aligned} \varphi \oplus \mathbf{v} &\mapsto (\varphi + \frac{d}{2} v_{h+n}) \oplus (\mathbf{v} - d\hat{\mathbf{e}}_h), \\ \varphi \oplus \mathbf{v} &\mapsto (\varphi + \frac{d}{2} v_h) \oplus (\mathbf{v} - d\hat{\mathbf{e}}_{n+h}), \end{aligned} \quad (34)$$

as the vectors on the left and right all represent the same Pauli operator  $\tau^{-2\varphi} W_{\mathbf{v}}$ . (This is used implicitly in the algorithm for determining distributions of measurement outcomes in Section III D.) By subsequently reducing the phase coefficient modulo  $d$ , the entire vector may be reduced modulo  $d$ .

While the above transformations do preserve which Pauli operator is represented by a given Pauli vector, it does not preserve the symplectic inner product of the Weyl block with those of other Pauli vectors. To maintain an extended tableau while reducing Weyl coefficients modulo  $d$ , one must also update the phase correction block  $\Xi$ . Suppose that  $\varphi_j \oplus \mathbf{v}_j \oplus \Xi \hat{\mathbf{e}}_j$  is the  $j^{\text{th}}$  column of an extended tableau  $T_S$  which represents a set of operators  $\{S_1, \dots, S_j, \dots, S_\ell\}$ . As with the operation to represent multiplication of generators described in Section IV A 1, we may reduce the  $h^{\text{th}}$  coefficient of  $\mathbf{v}$  by  $d$  by combining the phase correction information of the vector  $0 \oplus d\hat{\mathbf{e}}_h$  for the other generators  $S_1, \dots, S_\ell$ , to the vector  $\xi$  describing the phase correction information of  $\varphi \oplus \mathbf{v}$ . That is, we compute the row vector

$$\begin{aligned} \tilde{\xi}_h &= \frac{1}{2} \left[ [d\hat{\mathbf{e}}_h, \mathbf{v}_1] \quad \dots \quad [d\hat{\mathbf{e}}_h, \mathbf{v}_\ell] \right] \\ &\equiv \frac{d}{2} \hat{\mathbf{e}}_h^\top [\mathbf{0} \mid \sigma_{2n} \mid \mathbf{0}] T_S \pmod{d}, \end{aligned} \quad (35)$$

and then add  $\tilde{\xi}_h$  to the  $j^{\text{th}}$  row of the phase correction block  $\Xi$  (updating the phase correction information for all other columns with respect to the  $j^{\text{th}}$  column), and subtract  $\tilde{\xi}_h^\top$  from  $\xi$  (updating the phase correction information for the  $j^{\text{th}}$  column itself). Note that by subtracting  $\tilde{\xi}_h^\top$  from  $\xi$ , the phase correction necessary for

$\mathbf{v}$  is added into the  $j^{\text{th}}$  coefficient of  $\xi$ ; before updating the  $j^{\text{th}}$  row of the entire phase correction block, we may apply the superoperator  $\Psi_{j,j}$  to perform the necessary phase correction in the  $j^{\text{th}}$  column. As the coefficients of the phase correction block are only ever added to the phase coefficients, they may themselves always be reduced modulo  $d$  as in Eq. (35); thus whether the vector  $\tilde{\xi}_h$  and its transpose are added or subtracted is immaterial, except to maintain the antisymmetric property of the phase correction block. Thus, to reduce the  $(h, j)$  coefficient of the Weyl block of an extended stabilizer tableau for  $1 \leq h \leq n$  and obtain a new tableau  $\bar{T}'_S$ , we compute

$$\begin{aligned} \bar{T}'_S &= \Psi_{j,j} \left( T_S + \hat{\mathbf{e}}_{2n+1+j} \tilde{\xi}_h \right) \\ &\quad - (0 \oplus \mathbf{0} \oplus \tilde{\xi}_h^\top) \hat{\mathbf{e}}_j^\top - d \hat{\mathbf{e}}_{1+h} \hat{\mathbf{e}}_j^\top \\ &= \Psi_{j,j} \left( T_S + \frac{d}{2} \hat{\mathbf{e}}_{2n+1+j} \hat{\mathbf{e}}_{n+1+h}^\top T_S \right) \\ &\quad - \frac{d}{2} (0 \oplus \mathbf{0} \oplus [T_S^\top \hat{\mathbf{e}}_{n+1+h}]) \hat{\mathbf{e}}_j^\top - d \hat{\mathbf{e}}_{1+h} \hat{\mathbf{e}}_j^\top; \quad (36a) \end{aligned}$$

to reduce the  $(h+n, j)$  coefficients of the Weyl block for  $1 \leq h \leq n$ , we instead compute

$$\begin{aligned} \bar{T}'_S &= \Psi_{j,j} \left( T_S + \hat{\mathbf{e}}_{2n+1+j} \tilde{\xi}_h \right) \\ &\quad - (0 \oplus \mathbf{0} \oplus \tilde{\xi}_h^\top) \hat{\mathbf{e}}_j^\top - d \hat{\mathbf{e}}_{n+1+h} \hat{\mathbf{e}}_j^\top \\ &= \Psi_{j,j} \left( T_S + \frac{d}{2} \hat{\mathbf{e}}_{2n+1+j} \hat{\mathbf{e}}_{1+h}^\top T_S \right) \\ &\quad - \frac{d}{2} (0 \oplus \mathbf{0} \oplus [T_S^\top \hat{\mathbf{e}}_{1+h}]) \hat{\mathbf{e}}_j^\top - d \hat{\mathbf{e}}_{n+1+h} \hat{\mathbf{e}}_j^\top. \quad (36b) \end{aligned}$$

In both cases, the mapping is an affine superoperator, involving both the superoperator  $\Psi$  and transposition of the matrix  $T_S$ , and also of course the translation operation by  $-d \hat{\mathbf{e}}_{1+h} \hat{\mathbf{e}}_j^\top$  or  $-d \hat{\mathbf{e}}_{n+1+h} \hat{\mathbf{e}}_j^\top$  to reduce the actual coefficient of the tableau.

### 3. Fixing the number of rows of extended stabilizer tableaux

When simulating unitary transformations on states represented by extended stabilizer tableaux, it may be preferable to use linear operators of a fixed size, independently of the state being transformed. While the phase correction block is a square symmetric matrix, and may have a variable number of rows, we may bound its size if we can establish a maximum number of generators needed to describe an arbitrary stabilizer group. We can then pad the number of rows or columns in any tableau on  $n$  qudits to obtain tableaux with a fixed size.

As noted in Refs. [9, 16], a stabilizer group on  $n$  qudits may have a minimal generating set strictly larger than  $n$  when  $d$  is composite. The simplest example is the single-qudit state  $\frac{1}{\sqrt{2}}(|0\rangle + |2\rangle)$  described above for  $d = 4$ , for which  $\{Z^2, X^2\}$  is a minimal set of generators. (Similar examples exist for any composite  $d > 2$ ; one may consider a state stabilized by  $\{Z^{d_1}, X^{d_2}\}$  for arbitrary  $d_1, d_2 > 1$

on qudits of dimension  $d = d_1 d_2$ .) However, we may show that a minimal generating set for any  $n$ -qudit stabilizer group has at most  $2n$  generators, as follows. For any extended stabilizer tableau  $\bar{T}_S$  (proper or otherwise) with  $\ell > 2n$  columns, the Smith normal form  $S_S = L W_S R$  of its Weyl block  $W_S$  has the form

$$S_S = \left[ \begin{array}{cccc|c} t_1 & 0 & \cdots & \cdots & 0 \\ 0 & t_2 & & & \vdots \\ \vdots & & \ddots & & \vdots \\ \vdots & & & t_{2n-1} & 0 \\ 0 & \cdots & \cdots & 0 & t_{2n} \end{array} \right] \mathbf{0} \quad (37)$$

where each coefficient  $t_j$  is either zero or a divisor of  $D$ , and where  $t_{j+1}$  is a multiple of  $t_j$  for each  $j < 2n$ . The right-most  $(\ell - 2n)$  columns of  $W_S R$  are then also zero. Interpreting  $R$  as a recombination of the columns (and applying the appropriate phase corrections via Eq. (31a)), we obtain an extended tableau  $\bar{T}'_S$  which has  $W_S R$  as a Weyl block. The right-most  $(\ell - 2n)$  columns then each represent the identity operator, and may be omitted to leave a tableau with at most  $2n$  columns. As the phase correction block requires only as many rows as columns, we may specify an arbitrary stabilizer group with an extended stabilizer tableau having at most  $4n+1$  rows: one for the phase block, and  $2n$  each for the Weyl and phase-correction blocks. Thus, by padding, we may fix extended tableaux for  $n$  qudit states to have  $4n+1$  rows and  $2n$  columns.

### B. Simulating unitary stabilizer circuits on extended tableaux

We may extend conjugation tableaux, representing the effect of conjugation of Pauli operators by Clifford operators, very simply. As symplectic transformations do not affect the pair-wise symplectic inner products of the vectors  $\mathbf{v}_j$ , we may leave the phase correction blocks of the vectors  $\bar{\mathbf{p}}_j$  untouched when we describe a transformation by  $U \in \mathcal{C}_n(d)$ . An extended conjugation tableau corresponding to a conjugation tableau  $\mathcal{T}_U$  can thus be given by a square matrix

$$\bar{\mathcal{T}}_U = \left[ \begin{array}{c|c} \mathcal{T}_U & \mathbf{0} \\ \hline \mathbf{0} & \mathbb{1}_{2n} \end{array} \right] = \left[ \begin{array}{c|ccc|ccc} 1 & h_1 & \cdots & h_{2n} & 0 & \cdots & 0 \\ \hline 0 & & & & & & \\ \vdots & & C_U & & & & 0 \\ \hline 0 & & & & & & \\ \vdots & & & 0 & & \mathbb{1}_{2n} & \\ \hline 0 & & & & & & \end{array} \right], \quad (38)$$

where again  $C_U$  is a symplectic transformation of  $\mathbb{Z}_D^{2n}$ .

Simulating terminal measurements as in Section III D requires only the ability to compute alternative generating sets for the stabilizer group as described in Eq. (31a), and the ability to compute symplectic inner products as in Eq. (23). For the latter, symplectic inner products of

pairs of operators  $\mathbf{v}_h, \mathbf{v}_j$  are not pertinent for computing the inner products  $[\mathbf{p}, \mathbf{v}_h]$  and  $[\mathbf{p}, \mathbf{v}_j]$  which are necessary to determine the statistics for measuring an observable  $P = \tau^{-2\varphi} W_{\mathbf{p}}$ . Thus it suffices to compute the smallest integer  $s \geq 1$  such that

$$s \mathbf{p}^\top \left[ \begin{array}{c|c|c} \mathbf{0} & \sigma_{2n} & 0 \end{array} \right] \bar{T}_S \equiv \mathbf{0}^\top \pmod{d} \quad (39)$$

as a simple modification of Eq. (23). We may then carry out a simple variation of analysis of Section III D: defining  $\tilde{\xi}_h$  as in Eq. (35), we extend the tableau  $\bar{T}_S$  with vectors  $\tilde{\mathbf{u}}_h = 0 \oplus d\hat{\mathbf{e}}_h \oplus \tilde{\xi}_h^\top$  for  $1 \leq j \leq 2n$  in place of the vectors  $\mathbf{u}_h$  and  $\mathbf{u}'_h$  described in Section III D, and attempt to clear the Weyl block of the vector  $-(0 \oplus s\mathbf{p} \oplus \mathbf{0})$ , using Eq. (31a) to perform column combinations.

Adopting these extensions to stabilizer tableaux and conjugation tableaux allow us to simulate arbitrary stabilizer states, whose stabilizer groups may or may not be representable by a proper tableau, using linear operations over  $\mathbb{Z}_D$  as in Section III.

### C. Simulating stabilizer state evolution under Pauli measurements

In many cases, including the case  $d = 2$  and  $d$  odd, every stabilizer state has a proper tableau, and simulating Pauli measurements in general may be achieved by transformations of proper tableaux. However, for  $d > 2$  even, such measurements may transform a state from one which can be represented by a proper stabilizer tableau, to one which cannot. For instance, in the case  $d = 4$ , we may prepare the state

$$\begin{aligned} |\psi\rangle &= \Lambda X_{a,b}^2 F_a |0\rangle_a |0\rangle_b \\ &= \frac{1}{2}(|0\rangle + |2\rangle)_a \otimes |0\rangle_b + \frac{1}{2}(|1\rangle + |3\rangle)_a \otimes |2\rangle_b, \end{aligned} \quad (40)$$

for which we may easily construct a proper tableau using the techniques of Section III. However, if we measure  $Z_b$  on  $|\psi\rangle$ , the post-measurement state on  $a$  would differ from  $\frac{1}{\sqrt{2}}(|0\rangle + |2\rangle)$  by at most an  $X$  operation. As we saw in Section IV A, such states have no proper stabilizer tableaux. We must therefore extend the formalism of Section III to deal with evolution of states under measurement in the general case.

We now describe a procedure to describe this evolution for all  $d \geq 2$ , using the extended tableaux introduced in Section IV A, deferring the proofs of certain statements to Appendix B. (In Section IV C 3, we describe how this analysis may be simplified in the cases  $d = 2$  and  $d$  odd, for which extended tableaux are not in fact needed.) Using the constructions of Sections III C and IV B, we may reduce the problem to that of describing the effect of a single-qudit  $Z$  measurement. (Again, this has the side-effect of allowing us to simulate classically controlled Pauli operations depending on the measurement result using a coherent controlled-Pauli operator. We sketch a more direct approach to measurement in Section IV C 3.)

Let  $\mathcal{S} = \{S_1, \dots, S_\ell\}$  be a minimal generating set for a stabilizer group  $G_S$  which has a unique joint  $+1$ -eigenstate. A  $Z_r$  measurement has a non-trivial effect on a stabilizer state, and a non-deterministic outcome, if and only if the state is stabilized by a Pauli operator that does not commute with  $Z_r$ . Given an extended stabilizer tableau  $\bar{T}_S$ , we may compute whether  $Z_r$  commutes with each operator  $S_k \in \mathcal{S}$  by computing

$$\phi = \hat{\mathbf{e}}_r^\top \left[ \begin{array}{c|c|c} \mathbf{0} & \sigma_{2n} & 0 \end{array} \right] \bar{T}_S = (0 \oplus \hat{\mathbf{e}}_{n+r} \oplus \mathbf{0})^\top \bar{T}_S \quad (41)$$

following the description in Eq. (39). The result is a row-vector  $\phi = [\phi_1 \dots \phi_\ell] \in \mathbb{Z}_D^\ell$  such that  $Z_r S_k = \tau^{2\phi_k} S_k Z_r$ . As the row-vector  $\phi$  is the  $(n+r+1)^{\text{st}}$  row of the tableau  $\bar{T}_S$ , the tableau has the following block structure:

$$\bar{T}_S = \left[ \begin{array}{ccc|l} T_{1,1} & \cdots & T_{1,\ell} & \leftarrow \text{row 1} \\ T_{2,1} & \cdots & T_{2,\ell} & \leftarrow \text{row 2} \\ \vdots & & \vdots & \vdots \\ \phi_1 & \cdots & \phi_\ell & \leftarrow \text{row } n+r+1 \\ \vdots & & \vdots & \vdots \\ T_{2n+1,1} & \cdots & T_{2n+1,\ell} & \leftarrow \text{row } 2n+1 \\ \hline & \Xi_S & & \leftarrow \text{phase correction block} \end{array} \right] \quad (42)$$

We may recombine the generators described by the columns using Eq. (31a), to obtain a tableau  $\bar{T}_{\tilde{S}}$  which has at most one column — without loss of generality, the  $\ell^{\text{th}}$  column — containing an entry  $\eta \not\equiv 0 \pmod{d}$  in the  $(n+r+1)^{\text{st}}$  row:

$$\bar{T}_{\tilde{S}} = \left[ \begin{array}{ccc|c|l} \tilde{T}_{1,1} & \cdots & \tilde{T}_{1,\ell-1} & \tilde{T}_{1,\ell} & \leftarrow \text{row 1} \\ \tilde{T}_{2,1} & \cdots & \tilde{T}_{2,\ell-1} & \tilde{T}_{2,\ell} & \leftarrow \text{row 2} \\ \vdots & & \vdots & \vdots & \vdots \\ 0 & \cdots & 0 & \eta & \leftarrow \text{row } n+r+1 \\ \vdots & & \vdots & \vdots & \vdots \\ \tilde{T}_{2n+1,1} & \cdots & \tilde{T}_{2n+1,\ell-1} & \tilde{T}_{2n+1,\ell} & \leftarrow \text{row } 2n+1 \\ \hline & \Xi_{\tilde{S}} & & & \vdots \end{array} \right] \quad (43)$$

We may restrict  $\eta$  to be a divisor of  $d$  if it is non-zero, by multiplying the  $\ell^{\text{th}}$  column by a suitable scalar  $\alpha \in \mathbb{Z}_D^*$ . (To maintain the antisymmetry of the phase correction block, the  $\ell^{\text{th}}$  row of  $\Xi$  must also be multiplied by  $\alpha$  in this case.) Note that  $\eta \in \{0, 1, 2\}$  in the case that  $d = 2$ ,  $\eta \in \{0, 1\}$  in the case that  $d$  is an odd prime, and  $\eta \in \{0, d\}$  for any  $d \geq 2$  in the case that  $Z_r$  commutes with every generator of  $\mathcal{S}$ .

The tableau  $\bar{T}_{\tilde{S}}$  describes generators  $\tilde{\mathcal{S}} = \{\tilde{S}_1, \dots, \tilde{S}_\ell\}$  for  $G_S$  in which only  $\tilde{S}_\ell$  may fail to commute with the observable  $Z_r$ , depending on the precise value of  $\eta$ . Let  $\tilde{\mathbf{v}}_j$  represent the Weyl block of the  $j^{\text{th}}$  column of  $\bar{T}_{\tilde{S}}$ , and let  $s = d/\eta$  (if  $\eta > 0$ ), or  $s = 1$  (if  $\eta = 0$ ). Then  $s \geq 1$  is the smallest power of  $\tilde{S}_\ell$  such that  $\tilde{S}_\ell^s$  commutes with  $Z_r$ , as  $[s\tilde{\mathbf{v}}_\ell, \hat{\mathbf{e}}_r] \equiv 0 \pmod{d}$  by construction. Similarly,  $Z_r^s$  commutes with  $\tilde{S}_\ell$ , and thus with every element of  $\tilde{\mathcal{S}}$ .

### 1. Computing the distribution of measurement outcomes

As  $G_s$  stabilizes a unique state, it follows (by Lemma 12) that  $Z_r^s$  is proportional to some element of  $G_s$ . We introduce the vector

$$\xi = \frac{1}{2}s\phi^\top = \begin{cases} -\frac{d}{2}\hat{\mathbf{e}}_\ell, & \text{if } d \text{ is even and } \eta > 0; \\ \mathbf{0}, & \text{if } d \text{ is odd or } \eta = 0, \end{cases} \quad (44)$$

for the sake of brevity. This vector then contains the phase correction information needed in order to represent products of  $Z_r^s$ , which we represent by the Pauli vector  $(0 \oplus s\hat{\mathbf{e}}_r)$ , with the generators  $\tilde{S}_j$  in an extended tableau. We find the element of  $G_s$  to which  $Z_r^s$  is proportional using a similar technique to Section IV B, temporarily adjoining columns  $\hat{\mathbf{u}}_h = 0 \oplus d\hat{\mathbf{e}}_h \oplus \tilde{\xi}_h^\top$  for  $\tilde{\xi}_h$  as given in Eq. (35) to aid in performing column reduction on the tableau, using Eq. (31a) to perform column recombinations, to clear the Weyl block of the vector  $-(0 \oplus s\hat{\mathbf{e}}_r \oplus \xi)$ . The result will be some vector  $t \oplus \mathbf{0} \oplus \mathbf{0}$ ; by linearity, it follows that the operator

$$\tilde{R} := \tau^{-2t}Z_r^s = \tau^{-2t}W_{s\hat{\mathbf{e}}_r}, \quad (45)$$

represented by the extended Pauli vector  $t \oplus s\hat{\mathbf{e}}_r \oplus \xi$ , is the operator which is proportional to  $Z_r^s$  and contained in  $G_s$ . As in Section III D, the coefficient  $t$  must be a multiple of  $s$  in order for  $\tilde{R}$  to have a non-trivial  $+1$ -eigenspace. Because  $\tilde{R}$  commutes with  $G_s$  and with  $Z_r$ , it stabilizes both the pre-measurement and the post-measurement state. The operator  $R = \tau^{-2h_{\ell+1}}Z_r$  which stabilizes  $r$  after measurement satisfies  $R^s = \tau^{-2hs}Z_r^s = \tilde{R}$ ; that is, the measurement outcome  $h$  must satisfy  $h_{\ell+1} \equiv t/s \pmod{\eta}$ , or  $h_{\ell+1} \in t/s + \eta\mathbb{Z}_d$ . We may show (see Appendix B 3) that the outcome is in fact uniformly distributed among the residues modulo  $d$  satisfying this constraint.

In the case  $s = 1$  (i.e. if  $\eta \in \{0, d\}$ ), the state is stabilized by some operator  $\tau^{-2h}Z_r$  prior to measurement; the outcome is then a delta-peaked distribution, or “uniformly distributed” across the coset  $h + \eta\mathbb{Z}_d = \{h\} \subset \mathbb{Z}_d$ . Furthermore, the measurement of  $Z_r$  does not affect the state of the system; as an alternative to the above, we may transform the tableau to explicitly represent the fact that some operator  $\tau^{-2h}Z_r$  stabilizes the pre-measurement state by column-reduction, using the operations for column combinations and reduction modulo  $d$  of Sections IV A 1 and IV A 2. The resulting tableau will contain a column of the form  $h \oplus \hat{\mathbf{e}}_r \oplus \tilde{\xi}$  explicitly representing the operator  $\tau^{-2h}Z_r$ .

### 2. Computing and transforming between post-measurement states

Having fixed a given outcome  $h_{\ell+1}$  of the  $Z_r$  measurement, we perform the following transformations on  $\bar{T}_{\tilde{S}}$  to represent the post-measurement state. As the state is

unchanged if  $Z_r$  commutes with all stabilizer generators, we restrict ourselves to the case  $s > 1$ .

As  $\tilde{S}_\ell$  does not commute with  $Z_r$ , it does not stabilize the post-measurement state. But by construction,  $\tilde{S}_\ell^s$  does. To represent this, we multiply the  $\ell^{\text{th}}$  column of  $\bar{T}_{\tilde{S}}$  by  $s$ . To keep the phase correction block consistent, we multiply the  $\ell^{\text{th}}$  row of the phase correction block by  $s$  as well. We then augment the generating set to include the operator  $R$  stabilizing the measured qudit: we do so by replacing the adjoined  $(\ell + 1)^{\text{st}}$  column of the tableau with  $h_{\ell+1} \oplus \hat{\mathbf{e}}_r \oplus \xi$ . (Note that by construction,  $\xi$  as given in Eq. (44) is also the appropriate phase correction vector in this case). We must also extend the phase-correction block by an additional row to represent the new generator of the stabilizer group; by symmetry, this is simply  $\frac{d}{2}\hat{\mathbf{e}}_\ell^\top$  if  $d$  is even, or  $\mathbf{0}^\top$  for  $d$  odd. This yields a new extended tableau  $\bar{T}_{\tilde{S}'}$  representing a set  $\mathcal{S}'$  of stabilizer generators for the new state.

It may occur that the operator  $\tilde{S}_\ell^s$  represented by the  $\ell^{\text{th}}$  column of  $\bar{T}_{\tilde{S}'}$  is in fact  $\mathbb{1}$ , having a Weyl block consisting only of multiples of  $d$ . This will occur for instance if  $\eta = 1$  (which always occurs in the familiar case of  $d$  prime). If this is the case, we may drop the  $\ell^{\text{th}}$  column of the new tableau entirely, and over-write the  $\ell^{\text{th}}$  row of the phase correction block with the  $(\ell + 1)^{\text{st}}$  row rather than filling a new row. More generally, it may be the case that  $\tilde{S}_\ell^s$  can be generated by the other operators  $\{S'_1, \dots, S'_{\ell-1}, S'_{\ell+1}\} \subset \mathcal{S}'$ ; this necessarily occurs when  $\ell = 2n$ , as this is the maximum number of operators needed to generate the group  $G_{\mathcal{S}'}$ . To discover whether this is the case, we may attempt to clear the Weyl block of the  $\ell^{\text{th}}$  column of  $\bar{T}_{\tilde{S}'}$  modulo  $d$  (i.e. reduce it to a  $\{0, d\}$ -vector), as always using column operations with phase corrections as in Eq. (31a). If successful, the resulting vector in the  $\ell^{\text{th}}$  column represents the identity, and may be discarded as described above.

To simulate the transformation which occurs for a particular measurement outcome  $h^* \in t/s + \eta\mathbb{Z}_d$ , we may simply set  $h_{\ell+1} := h^*$  by fiat, and perform the operations as above. In a physical setting with actual stabilizer circuits acting on qudits of dimension  $d$ , as in the familiar case  $d = 2$ , one may simulate fixing the outcome by transforming the post-measurement state unitarily between the possible outcomes. For  $d \geq 2$  arbitrary, we may show that it suffices to act on the post-measurement state with the operator  $\tilde{S}_\ell$ , which is represented by conjugating each of the elements of  $\mathcal{S}'$  by  $\tilde{S}_\ell$ . By construction, this operator commutes with the generators  $S'_j = \tilde{S}_j$  for  $1 \leq j < \ell$ , as well as the generator  $S'_\ell = \tilde{S}_\ell^s$ , which are represented by the first  $\ell$  columns of the tableau  $\bar{T}_{\tilde{S}}$ ; it only fails to commute with the generator  $S'_{\ell+1} = R \propto Z_r$ , transforming it to  $R' = \tau^{-2\eta}R = \tau^{-2(h_{\ell+1} + \eta)}Z_r$  instead. Repeated applications of powers of  $\tilde{S}_\ell$  then suffice to produce any desired post-measurement state by adding a suitable multiple of  $\eta$  to the exponent in the phase.

The entirety of the above analysis, for non-commuting  $Z_r$  measurements, generalizes the well-known stabilizer

formalism in prime dimension (as in Ref. [8]). If  $d$  is prime, we have  $\eta = 1$  as we have noted above, so that the post-measurement state is no longer stabilized by  $\tilde{S}_\ell$  but instead by  $R = \tau^{-2h} Z_r$ , for some  $h$  uniformly distributed over  $\mathbb{Z}_d$ . The novel features for  $d$  arbitrary are that the possible outcomes over which  $h$  varies can in general be any coset of the form  $\kappa + \eta\mathbb{Z}_d$  (which is equal to the whole group  $\mathbb{Z}_d$  only when  $\eta = 1$ ), and that the post-measurement state is still stabilized by  $\tilde{S}_\ell^{d/\eta}$  (which is trivial only when  $\eta = 1$ ).

### 3. Special cases permitting simplified evolution under measurements

The extensions of the preceding sections to the stabilizer formalism allow us to simulate arbitrary stabilizer circuits for arbitrary dimensions  $d \geq 2$ . We now briefly remark on simplifications which are possible in some special cases, which may lead to modest savings in the amount of effort and work-space required in practice.

When simulating a measurement of a Pauli operator  $P = \tau^{-2\delta} W_{\mathbf{p}}$ , it may be that no further operations depend on the measurement outcome (*i.e.* on the eigenvalue  $\tau^{2h}$  corresponding to the post-measurement state); or if the outcome is used only to control Clifford operations, that representing the outcome by the state of a qudit provides no advantage. In either case, the introduction of an explicit measurement register for controlled-Pauli operators to act upon is unnecessary. We may compute the distribution of outcomes, and the post-measurement state conditioned on any particular outcome, in a similar way as described above but without the introduction of a measurement register. Elaborating Eq. (41), we compute

$$\phi = (0 \oplus \mathbf{p} \oplus \mathbf{0})^\top \bar{T}_S, \quad (46)$$

and consider whether it is equivalent to zero modulo  $d$ ; if not, we consider what reversible column-transformation operations would map it to a row-vector of the form  $\eta \hat{\mathbf{e}}_\ell^\top$ , and then apply those same transformations to the tableau  $T_S$ . Doing so yields a tableau representing a generating set  $\tilde{S} = \{\tilde{S}_1, \dots, \tilde{S}_\ell\}$  in which only  $\tilde{S}_\ell$  fails to commute with  $P$ ; one may easily generalize the analysis above from that point on, substituting the Pauli vector  $(0 \oplus \hat{\mathbf{e}}_r)$  representing  $Z_r$  with the vector  $(\delta \oplus \mathbf{p})$  representing  $P$ . Doing this is substantially similar to performing the same operations as in Section IV C 2, as performed on a tableau where we *have* simulated the  $P$  measurement by a  $Z_r$  measurement, with the primary difference being that we omit the additional column involved by explicitly introducing the ancilla  $r$ .

As noted in Section III A, extended stabilizer tableaus are unnecessary in the case of  $d$  either prime or odd, as all stabilizer groups may be represented in those cases by proper stabilizer tableaus. In the case of odd  $d$ , no special effort is necessary, as all stabilizer tableaus are proper in that case; we may omit phase correction blocks in that case. In the remaining case  $d = 2$  (*i.e.*, for qubits),

further effort is required to ensure that the tableau of a post-measurement state is proper if we are to dispense with phase correction blocks. If at least one of the elements of the stabilizer group  $G_S$  fails to commute with the Pauli operator  $P = \tau^{-2\delta} W_{\mathbf{p}}$  being measured, we may as usual obtain a generating set  $\{\tilde{S}_1, \dots, \tilde{S}_\ell\}$  in which exactly one generator  $\tilde{S}_\ell$  does not commute with  $P$ ; it suffices to compute a vector  $\tilde{\mathbf{p}} \equiv \mathbf{p} \pmod{2}$  such that  $P = \tau^{-2\delta} W_{\mathbf{p}} = \tau^{-2\delta} W_{\tilde{\mathbf{p}}}$ , which is orthogonal modulo  $D$  (where  $D = 4$  in this case) to the columns of the Weyl block  $W_S$  representing  $\tilde{S}_j$  for  $1 \leq j < \ell$ . We may compute  $\tilde{\mathbf{p}}$  using the techniques presented in Appendix A 1 in this case, which should have a single solution. If however  $P$  commutes with the entire stabilizer group, there is no choice in how it may be represented in order to maintain a proper tableau: an operator proportional to  $P$  is already generated by the group, and the system of equations in Appendix A 1 determining a suitable representative for that operator has a unique solution  $\tilde{\mathbf{p}}$ , for which  $[\tilde{\mathbf{p}}, \mathbf{p}] \equiv 2 \pmod{4}$  may hold. In this case, however, no transformation of the state occurs upon measurement, so the existing proper tableau suffices to describe the post-measurement state. We may then dispense with extended tableaus in these cases if desired (though extended tableaus still provide the benefit of making possible reduction of the coefficients modulo 2 for tableaus over qubits).

Finally, for  $d$  prime, certain elements of the analysis in Section III D and Section IV C may be simplified to yield the known results for simulations of measurements in those cases [8]. For instance, in the case that not all generators  $S_j \in S$  commute with the measurement operator  $P$ , it is not necessary to perform column transformations to obtain a column which represents an operator  $\tilde{S}_\ell$  such that  $[P, \tilde{S}_\ell] = \tau^{2\eta} = \tau^2$ . We may instead find any single operator  $S_j$  which fails to commute with  $P$ , and compute some non-trivial power  $S_j^t$  of it such that  $[P, S_j^t] = \tau^2$ , and use this to obtain a generating set in which only  $S_j^t$  fails to commute with  $P$  by combining other generators with appropriate powers of  $S_j^t$ . Also, no non-trivial power of  $S_j$  will be represented by the table  $T_{S'}$  for the post-measurement state; in particular, the tableau will never have more than  $n$  columns.

## V. COMPLEXITY OF SIMULATING STABILIZER CIRCUITS

The main benefit provided by the formalism of this paper above the existing techniques in the literature is that computing phases are effectively reduced to simple linear transformations, thereby simplifying the individual steps of simulating stabilizer circuits, which should reduce the burden of carrying out transformations in analytical investigation and ad-hoc calculations. (This is not to say that these operations are asymptotically more efficient: we remark on this distinction in Section V C.) However,

the reduction to linear algebra in itself also makes certain complexity theoretic results easier to prove, when considering computational complexity classes which themselves are well characterized in linear algebraic terms. Using the techniques of Sections III and IV, we generalize the results of Aaronson and Gottesman [11] concerning the complexity of simulating stabilizer circuits to qudits of arbitrary dimension. Specifically, natural decision problems concerning simulating stabilizer circuits on qudits of any fixed dimension  $d$ , involving at most a constant number of measurements, are complete for the complexity class  $\text{coMod}_d\mathbf{L}$  consisting of problems which are log-space reducible to determining whether a system of equations mod  $d$  is feasible [30]. We describe these results in this section.

#### A. Complexity of simulating unitary stabilizer circuits

We define DEFINITE STABILIZER MEASUREMENT to be the problem of deciding whether or not the state of a system of  $n$  qudits of dimension  $d$ , initially in a computational state  $|\mathbf{q}\rangle$  and then acted on by a unitary stabilizer circuit, is stabilized by some particular  $P \in \mathcal{P}_d^{\otimes n}$ . This is equivalent to the proposition that a measurement of the operator  $P$  would yield a record of “0” with certainty, being a  $+1$ -eigenstate of  $P$ . (Other possible outcomes  $h \in \mathbb{Z}_d$  may be considered instead by testing whether  $\tau^{-2h}P$  stabilizes the state.) If the outcome “0” does not occur with certainty, it occurs either with probability 0, or probability  $1/s$  (at most  $\frac{1}{2}$ ) for some integer  $s$  which divides  $d$ .

In the special case of a  $P = -Z_1$  measurement on qubits ( $d = 2$ ), DEFINITE STABILIZER MEASUREMENT corresponds to the problem GOTTESMAN-KNILL described by Aaronson and Gottesman [11]. This problem belongs to the class  $\oplus\mathbf{L}$  of problems which are log-space reducible to feasibility of systems of linear equations mod 2 and verifying coefficients of matrix products mod 2 [12]. Relying on the result  $\mathbf{L}^{\oplus} = \oplus\mathbf{L}$  [31], Aaronson and Gottesman describe an algorithm solving GOTTESMAN-KNILL on a logspace machine with access to an  $\oplus\mathbf{L}$  oracle, which is used to repeatedly simulate initial segments of the stabilizer circuit in order to compute the effects of the phase corrections induced on intermediate states of the circuit. We show a more direct and generalized version of the result of Ref. [11] by characterizing the complexity of DEFINITE STABILIZER MEASUREMENT.

Just as  $\oplus\mathbf{L}$  is the class of problems which are log-space reducible to verifying coefficients of matrix products modulo 2, we may define the class  $\text{coMod}_d\mathbf{L}$  as the class of decision problems which are log-space reducible to verifying coefficients of matrix products modulo  $d$  [14] (see note [32]). In particular, this implies  $\oplus\mathbf{L} = \text{coMod}_2\mathbf{L}$ . As Ref. [30] shows, testing whether a system of equations is feasible mod  $d$  is also a complete problem for  $\text{coMod}_d\mathbf{L}$  for all  $d \geq 2$ ; and in the particular case where  $d$  is a prime

power,  $\text{coMod}_d\mathbf{L}$  may be characterized as those problems which are log-space reducible to *evaluating* (as opposed to *verifying*) coefficients of matrix products modulo  $d$ . These operations are in essence precisely what is required to simulate the transformations of a stabilizer tableau in a unitary stabilizer circuit, so that we may show:

**Theorem 7:** For qudits of some fixed dimension  $d \geq 2$ , DEFINITE STABILIZER MEASUREMENT is complete for the class  $\text{coMod}_d\mathbf{L}$ .

**Proof:** As in the analysis of Section IIID, determining whether an  $n$ -qudit state, characterized by a (proper) stabilizer tableau  $T_f$ , is stabilized by an operator  $P = \tau^{-2\delta}W_{\mathbf{p}}$  corresponds to determining whether there is a vector  $\delta' \oplus \mathbf{p}'$  in the column-span of  $T_f$  such that  $P = \tau^{-2\delta'}W_{\mathbf{p}'}$ . This may be reduced to determining whether there is a solution to some system of equations  $A\mathbf{t} \equiv (\delta \oplus \mathbf{p}) \pmod{D}$  for some matrix  $A$ :

- For  $d$  odd, in order for  $P = \tau^{-2\delta'}W_{\mathbf{p}'}$ , we require that  $\mathbf{p}' - \mathbf{p} \equiv 0 \pmod{d}$ , and that  $2\delta' - 2\delta \equiv [\mathbf{p}', \mathbf{p}] \equiv 0 \pmod{d}$ , so that  $\delta \oplus \mathbf{p}$  is in the column span of  $T_f$ . We then set  $A := T_f$ .
- For  $d$  even, we still require  $\mathbf{p}' - \mathbf{p} \equiv 0 \pmod{d}$ , but this is no longer sufficient to ensure  $\mathbf{p} = \mathbf{p}' \in \mathbb{Z}_D$ ; and again we require  $2\delta' - 2\delta \equiv [\mathbf{p}', \mathbf{p}] \equiv 0 \pmod{D}$ . Then  $\mathbf{p}' - \mathbf{p} = d\mathbf{x}$  for some  $\mathbf{x} \in \{0, 1\}^{2n}$ , and  $\delta' = \delta + \frac{1}{2}[\mathbf{p} + d\mathbf{x}, \mathbf{p}] = \frac{d}{2}[\mathbf{x}, \mathbf{p}] \pmod{d}$ . The vector  $d\mathbf{x}$  corresponds to some representation of the identity operator  $\mathbb{1} = W_{d\mathbf{x}}$  which accounts for the difference in the phase coefficients, by the formula

$$\begin{aligned} \tau^{-2\delta'}W_{\mathbf{p}'} &= \tau^{-2\delta + [d\mathbf{x}, \mathbf{p}]}W_{\mathbf{p} + d\mathbf{x}} \\ &= \tau^{-2\delta}W_{\mathbf{p}}W_{d\mathbf{x}}, \end{aligned} \quad (47)$$

by Lemma 2. As in Section IIID, we introduce auxiliary columns of the form  $\mathbf{u}_0 = d \oplus \mathbf{0}$  and  $\mathbf{u}_j := \frac{d}{2}[\hat{\mathbf{e}}_j, \mathbf{p}] \oplus d\hat{\mathbf{e}}_j$  for  $1 \leq j \leq 2n$  to the tableau  $T_f$ , chosen so that  $\mathbf{u}_j + (\delta \oplus \mathbf{p})$  also represents the operator  $P$  for each  $0 \leq j \leq 2n$ . Thus, it suffices to determine whether the system of equations  $A\mathbf{t} = [\mathbf{u}_0 \ \mathbf{u}_1 \ \cdots \ \mathbf{u}_{2n} \mid T_f] \mathbf{t} = (\delta \oplus \mathbf{p})$  has solutions modulo  $2d$ .

In each case, to test the feasibility of such a system of equations has solutions with a  $\text{coMod}_d\mathbf{L}$  algorithm, it is not necessary to store  $T_f$  explicitly in the workspace; it suffices to be able to efficiently query individual coefficients of  $T_f$  on demand, using only  $O(\log(n))$  workspace.

In the case where  $T_f$  represents a stabilizer state  $U|\mathbf{q}\rangle$  obtained by acting on a standard basis state  $|\mathbf{q}\rangle \in \mathcal{H}_d^{\otimes n}$  with a Clifford operator  $U \propto U_N \cdots U_2 U_1$ , we define  $T_f$  as the action of a sequence of operators  $\bar{C}_N \cdots \bar{C}_2 \bar{C}_1$  acting on an initial tableau of the form  $T_0 := [\mathbf{q} \mid 0]^\top$ , where each  $\bar{C}_j$  is a conjugation tableau as in Eq. (12). We then consider two cases:

- Suppose  $d = p^e$  for some prime  $p$ . Using the techniques of Ref. [30], for any prime power  $p^e$ , we may compute the coefficients of such a matrix product modulo  $p^e$  as part of a  $\text{coMod}_p\text{L}$  algorithm. Determining whether the system of equations  $\mathbf{A}\mathbf{t} \equiv (\delta \oplus \mathbf{p})$  is feasible modulo each prime-power divisor  $p^e$  is thus in  $\text{coMod}_p\text{L}$ .
- For qudit dimensions having a prime power decomposition  $d = p_1^{e_1} \cdots p_\ell^{e_\ell}$  for  $\ell > 1$ , note that  $\mathbf{A}\mathbf{t} \equiv (\delta \oplus \mathbf{p}) \pmod{D}$  is feasible if and only if  $\mathbf{A}\mathbf{t} \equiv (\delta \oplus \mathbf{p}) \pmod{p^e}$  is also feasible for every prime-power factor  $p^e$  of  $D$ . Define the problem  $\mathbf{L}_d$  to be the problem DEFINITE STABILIZER MEASUREMENT for a fixed qudit dimension  $d$ . Then we may characterize  $\mathbf{L}_d$  as

$$\mathbf{L}_d = \mathbf{L}_{p_1^{e_1}} \cap \mathbf{L}_{p_2^{e_2}} \cap \cdots \cap \mathbf{L}_{p_\ell^{e_\ell}}. \quad (48)$$

By a standard normal form for  $\text{coMod}_d\text{L}$  [30, Prop. 3], it follows that  $\mathbf{L}_d \in \text{coMod}_d\text{L}$  if and only if  $\mathbf{L}_{p^e} \in \text{coMod}_{p^e}\text{L}$  ( $= \text{coMod}_p\text{L}$ ) for each prime power  $p^e$  which divides  $d$ .

Thus, DEFINITE STABILIZER MEASUREMENT for qudits of dimension  $d$ , is in  $\text{coMod}_d\text{L}$  for all integers  $d \geq 2$ . Finally, as simulating circuits consisting only of  $\Lambda\text{X}$  gates on qudits of dimension  $d$  is itself  $\text{coMod}_d\text{L}$ -hard [33], it follows that DEFINITE STABILIZER MEASUREMENT for dimension- $d$  qudits is  $\text{coMod}_d\text{L}$ -complete.  $\square$

We may generalize further, to consider the complexity of the problem of computing the output distribution of a measurement of a given observable. For a given qudit dimension  $d$  and a probability distribution over  $\mathbb{Z}_d$ , define STABILIZER MEASUREMENT to be the problem of deciding whether this distribution can be produced by measuring a given observable  $P = \tau^{-2\delta} W_{\mathbf{p}}$  on the state produced by a specified unitary stabilizer circuit  $U$  acting on a given standard basis state  $|\mathbf{q}\rangle$ . We restrict the distributions taken as input to uniform distributions over a coset  $\kappa + \eta\mathbb{Z}_d \subseteq \mathbb{Z}_d$ , where  $\kappa, \eta \in \mathbb{Z}_d$  are parameters specifying the distribution. (The delta-peaked distributions of DEFINITE STABILIZER MEASUREMENT correspond to the case  $\eta = d$ , and testing whether  $\tau^{-2\kappa} P$  stabilizes the state  $U|\mathbf{q}\rangle$ ; the uniform distribution over all of  $\mathbb{Z}_d$  corresponds to  $\eta = 1$ , with  $\kappa$  being redundant.) Consider the proper tableau  $T_f$  just prior to measurement: by Section IIID, the outcome is uniformly distributed over  $\kappa + \eta\mathbb{Z}_d \subseteq \mathbb{Z}_d$  if and only if the row-vector  $\phi := (0 \oplus \mathbf{p})^\top T_f$  has the property that  $\eta = \gcd(d, \phi_1, \phi_2, \dots)$ , and the integer vector  $\frac{d}{\eta}[(\kappa - \delta) \oplus \mathbf{p}]$  is generated modulo  $D$  by the columns of  $T_f$  (together with auxiliary columns  $\mathbf{u}_j := \frac{d}{2}[\hat{\mathbf{e}}_j, \mathbf{p}] \oplus d\hat{\mathbf{e}}_j$  and  $\mathbf{u}_0 = d \oplus \mathbf{0}$  in the case of  $d$  even, as in the proof of Theorem 7). We may test both of these conditions by solving linear equations modulo  $D$ : this is obvious for the latter constraint, and we also have  $\eta = \gcd(d, \phi_1, \phi_2, \dots)$  if and only if the system of equations  $\eta \equiv \phi^\top \mathbf{x} \pmod{d}$  has solutions. As  $\text{coMod}_d\text{L}$  is closed

under logical conjunctions, STABILIZER MEASUREMENT is thus also complete for  $\text{coMod}_d\text{L}$ .

Note that STABILIZER MEASUREMENT is equivalent to determining whether the probability of obtaining a given outcome  $h$  is equal to  $1/s$  for some  $s > 1$ , as this holds if and only if the outcome is uniformly distributed over  $h + (d/s)\mathbb{Z}_d$ . We therefore have:

**Theorem 8:** For an initial state in the standard basis, any Pauli measurement observable  $P \in \mathcal{P}^{\otimes n}$ , and any stabilizer circuit which performs a  $P$  measurement, the following problems are all  $\text{coMod}_d\text{L}$ -complete: (a) verifying predictions of a deterministic measurement outcome  $h \in \mathbb{Z}_d$ , (b) verifying predictions of having probability  $p$  of obtaining an outcome  $h \in \mathbb{Z}_d$ , and (c) verifying predictions of the distribution of measurement outcomes.

As a corollary, all of the problems described above may be simulated by  $O(\log(n)^2)$ -depth boolean circuits, as  $\text{coMod}_d\text{L} \subseteq \text{NC}^2$  [14].

## B. The complexity of simulating stabilizer circuits with multiple measurements

We now consider the way in which the results of the preceding section extend to complexity containments for stabilizer circuits with measurements, *i.e.* in which the evolution of the state under measurement must be explicitly computed and where the outcomes may control further operations. To simulate the transformation of a state under measurement — as opposed to determining what the distribution of outcomes is, as in the STABILIZER MEASUREMENT problem — we must describe how a  $\text{coMod}_d\text{L}$  algorithm might carry out the calculations described in Section IV C.

### 1. Simulating evolution under a single measurement

We first sketch an algorithm to verify any single coefficient of an (extended) post-measurement tableau  $\bar{T}_{S'}$  in  $\text{coMod}_{p^e}\text{L}$ , for a qudit dimension of  $p^e$  for some prime  $p$ , where the measurement outcome is somehow specified in the input and where we assume we may query coefficients of the pre-measurement tableau  $\bar{T}_S$ . The tableau  $\bar{T}_{S'}$  is that which results from a  $Z_r$  measurement acting on a pre-measurement tableau  $\bar{T}_S$  via the procedure of Section IV C. The motivation for restricting to prime-power qudit dimension is to describe a solution involving query access to  $\bar{T}_S$ , which may be difficult to simulate in logarithmic space for composite  $d$ . We indicate how this extends to composite qudit dimensions  $d$ , in a manner similar to the proof of Theorem 7, before proceeding to the case of evolution under a sequence of measurements.

To evaluate a coefficient of the post-measurement tableau  $\bar{T}_{S'}$ , we do not have to store the entire tableau as it is transformed, so long as we can efficiently reconstruct



the dependencies of the coefficient in question on the coefficients of the pre-measurement tableau  $\bar{T}_S$  on demand. We therefore describe how to reproduce which transformations are performed on  $\bar{T}_S$ , and the impact of these transformations on the desired coefficient.

The transformations performed on a tableau consist largely of column recombinations to clear the  $(n+r+1)^{\text{st}}$  row of the tableau. These may be performed by invertible transformations, in which one column is added or subtracted from another some number of times; for a prime-power modulus, determining a combination in which the  $(n+r+1)^{\text{st}}$  coefficient of one of the columns is sent to zero is easy, using comparisons and divisions of fixed-size integers in  $\{0, 1, \dots, D-1\}$ . We may consider consecutive pairs of columns in turn — first considering combinations of the first column with the second column, then combinations of the second column with the third, and so on — and determine for each pair the transformation which will clear the  $(n+r+1)^{\text{st}}$  coefficient of the left-most column in each case. By considering the effect of this sequence of column-combinations on the coefficients in other rows, we may determine how the coefficients in those rows transform, in order to determine what the value of any one given coefficient of  $\bar{T}_{S'}$  would be. We may do this using enough workspace to store the  $(n+r+1)^{\text{st}}$  coefficients of whichever two columns we consider at each step of the algorithm, as well as the coefficients for the same two columns in any other row we require; and enough workspace to carry out simple calculations, such as division, on fixed-width integers. Apart from the column recombinations of the tableau, computing  $\eta$  (and the scalar factor  $\alpha$  by which we multiply the final non-zero column, as described following Eq. (43)) can be easily performed in constant space, as can  $s = d/\eta$  for  $\eta > 0$ .

In the case of a power of an odd prime, the above suffices to determine all the coefficients of the tableau  $\bar{T}_S$  which represents the same pre-measurement state as  $\bar{T}_S$ , in which only a single generator  $\tilde{S}_\ell$  fails to commute with  $Z_r$ . In the case of  $d$  even, the phase correction block and the phase vector both involve row operations for each column operation. For a phase coefficient, we must also query off-diagonal coefficients from the phase correction block of the tableau, as it is being transformed; then some additional workspace is required to compute these coefficients. A phase correction block coefficient itself may be subject to both column and row operations throughout the transformation of the stabilizer tableau: we may outline how these may be computed as follows. Suppose we wish to compute the value that the  $(h, j)$  coefficient of the phase correction block would have after performing the  $k^{\text{th}}$  round of column recombinations, where  $1 \leq h, j, k \leq 2n$ . The phase correction block is antisymmetric by construction, throughout the transformation of the tableau, which allows us to make the following observations:

- (i) If  $j = h$ , we return 0; and if  $j > h$ , we may instead compute the negation of the  $(j, h)$  coefficient of the phase correction block.

- (ii) If  $j < h$  and  $k < h - 1$ , then none of the row-transformations on the phase correction block corresponding to recombining the first  $k$  columns of the tableau have affected any coefficients in the  $h^{\text{th}}$  row of the phase correction block, in which case we may simply simulate the effect of the first  $k$  column combinations on the  $(h, j)$  coefficient of the phase correction block, as for the Weyl block coefficients. (In particular, if  $k < j - 1$ , we may simply return the corresponding coefficient of  $\bar{T}_S$ .)

- (iii) If  $j = k = h - 1$ , then the  $(h, j)$  coefficient is in principle affected by row-transformations between the  $(h - 1)^{\text{st}}$  row and the  $h^{\text{th}}$  row. However, as the  $(h - 1, h - 1)$  coefficient of the phase correction block is zero, this row-operation has no effect, and we may reduce to the preceding case.

- (iv) If  $j < h \leq k$ , the  $(h, j)$  coefficient of the phase block is affected by row-transformations which in general will have a non-trivial effect. We recursively compute coefficients  $b_{t,j}$  corresponding to the  $(t, j)$ -coefficient of the phase correction block after  $t$  column combinations, for  $j + 1 \leq t \leq h + 1$ . Starting by computing  $b_{j+1,j}$  as in the preceding case, we compute each subsequent  $b_{t,j}$  as follows: let  $b'_{t,j}$  be the value of the  $(t', j)$ -coefficient of the phase correction block after the first  $t - 2$  column combinations, and then simulate the appropriate row-transformations with  $b_{t-1,j}$  and  $b'_{t,j}$  to compute the value of  $b_{t,j}$  after the  $(t - 1)^{\text{st}}$  column combination.

All of the above can be performed in constant workspace, using at most two levels of recursive evaluation of the coefficients of the phase-correction block (as in the final case above).

Having obtained a tableau  $\bar{T}_S$  representing the pre-measurement group, for which only a single generator  $\tilde{S}_\ell$  fails to commute with  $Z_r$ , we may easily describe the remaining calculations required to determine coefficients of the tableau. The eigenvalue  $\tau^{2t}$  of the pre-measurement state with respect to the operator  $Z_r^s$  can be obtained by multiplying the measurement outcome specified for  $Z_r$  at the input by  $s$ ; we may then use a `coModpL` oracle to solve DEFINITE STABILIZER MEASUREMENT to determine whether the specified outcome is possible, and if so, proceed with the computation (perhaps returning an error value otherwise). The column  $t \oplus \hat{\mathbf{e}}_r \oplus \boldsymbol{\xi}$  describing the stabilizer arising from the measurement will be the  $(\ell + 1)^{\text{st}}$  column of the tableau, for  $\boldsymbol{\xi} \in \{0, \frac{d}{2}, d, \frac{3d}{2}\}$  as described in Eq. (44), unless the column vector representing the generator  $\tilde{S}_\ell^s$  can be expressed as a combination of  $t \oplus \hat{\mathbf{e}}_r \oplus \boldsymbol{\xi}$  together with the other columns, modulo  $p^e$ . We may determine this once more with a `coModpL` oracle to solve systems of equations; and if there is indeed a solution, we omit the column corresponding to the old generator  $\tilde{S}_\ell$  entirely.

As a minor variation of the procedure of Section IV C, we may switch the two columns representing the mea-

surement stabilizer  $\tau^{-2h}Z_r$  and the generator  $\tilde{S}_\ell^s$ , so that the former is always the  $\ell^{\text{th}}$  column and the latter the  $(\ell+1)^{\text{st}}$  column in the case that it is non-trivial. We may fix the number of columns to the maximum of  $2n$  as described in Section IV A 3, setting all additional columns to zero. All of the above suffice to compute any particular coefficient of the post-measurement tableau  $\bar{T}_{S'}$ , modulo  $p^e$ ; if a test-value for the coefficient is provided as input, we may then test congruence modulo  $p^e$  as well.

Using the characterization of  $\text{coMod}_d\mathbf{L}$  for arbitrary  $d \geq 2$  (possibly divisible by multiple primes) described in Ref. [30, Prop. 3], this suffices to verify coefficients of a tableau transformed under measurement for arbitrary qudit dimension as well. Any linear transformations which are invertible modulo the prime-power divisors  $p_1^{e_1}, p_2^{e_2}$ , etc. of  $D$  are also invertible modulo  $D$ , by the Remainder Theorem; therefore each of the column transformations modulo the prime powers  $p_j^{e_j}$  correspond to valid column transformations modulo  $D$  as well. By moving the column for the one generator of the group whose presence (or rather, whose status as a non-trivial generator) is uncertain to the  $(\ell+1)^{\text{st}}$  column, the columns in the tableaux for each prime-power divisor  $p_j^{e_j}$  correspond to the same generators as one another; any prime-power divisor  $p_j^{e_j}$  for which some generator corresponds to the zero vector merely represents a Pauli stabilizer which is proportional to some Weyl operator  $W_{p_j^{e_j}\mathbf{v}}$ . Thus, verifying the value of any given coefficient of a post-measurement tableau  $\bar{T}_{S'}$  for qudits of any dimension  $d \geq 2$  with respect to a  $Z_r$  measurement is a problem contained in  $\text{coMod}_d\mathbf{L}$ .

## 2. Simulating multiple measurements in arbitrary dimensions

From the foregoing, it is straightforward to use known oracle-closure results for prime-power  $d$  [31] to show that a stabilizer circuit involving any constant number of measurements may be simulated in  $\text{coMod}_d\mathbf{L}$ , for qudits of arbitrary dimension  $d \geq 2$ . We proceed again along the same lines as the preceding section, by bounding the complexity for qudits of prime-power dimension, and then lifting to arbitrary dimension  $d$ .

In the procedure above for simulating a measurement of a tableau in prime-power dimension  $p^e$ , we assumed the ability to query individual coefficients of the tableau  $\bar{T}_S$  which represents the pre-measurement state. Each coefficient of the post-measurement tableau may be evaluated in  $\text{coMod}_p\mathbf{L}$ , provided we supplement the computation with an oracle for the coefficients of  $\bar{T}_S$ . If  $\bar{T}_S$  arises from the simulation of a stabilizer circuit — which may also be simulated in  $\text{coMod}_p\mathbf{L}$  — it follows that properties of interest of the post-measurement tableau may be computed in  $\text{coMod}_p\mathbf{L}^{\text{coMod}_p\mathbf{L}}$ . If  $\bar{T}_S$  itself arises from a circuit which involves a single measurement, an oracle for evaluating coefficients of  $\bar{T}_S$  can be implemented using a  $\text{coMod}_p\mathbf{L}^{\text{coMod}_p\mathbf{L}}$  oracle, *i.e.* an oracle which itself

has access to an oracle to evaluate the coefficients of the tableau immediately following the first measurement.

Consider the problem of simulating a stabilizer circuit with  $k > 1$  measurements, in the sense of computing coefficients of the stabilizer tableau (possibly in order to determine whether a given outcome  $h_k \in \mathbb{Z}_d$  occurs for the final measurement), given some sequence of intermediate measurement outcomes  $h_1, \dots, h_{k-1} \in \mathbb{Z}_d$ . Generalizing the description above, the simplest way to regard the computational complexity of this problem is to provide one layer of nested  $\text{coMod}_p\mathbf{L}$  oracles for each measurement, yielding a hierarchy of oracles for simulating each successive measurement. Simulating a stabilizer circuit with  $k$  measurements is then contained by the class

$$\text{coMod}_p\mathbf{L}^{\text{coMod}_p\mathbf{L}^{\text{coMod}_p\mathbf{L}^{\dots}}}$$

with a tower of  $k-1$  oracles to simulate the first  $k-1$  measurements. For any fixed  $k > 1$  which is constant in the input size, this class is simply equal again to  $\text{coMod}_p\mathbf{L}$ , by the oracle closure results of Ref. [31] for  $p$  prime (but see note [34]). Thus simulating the outcomes of any fixed number of measurements can be simulated in  $\text{coMod}_p\mathbf{L}$  for qudit dimension  $p^e$ .

For arbitrary dimensions, as we remark in the proof of Theorem 7, the problem of simulating a stabilizer circuit on  $d$  dimensional qudits can be reduced to the corresponding problem for each prime-power factor  $p^e$  of  $d$ . For instance, to determine whether a sequence of  $k \in O(1)$  measurements yields outcomes  $h_1, \dots, h_k \in \mathbb{Z}_d$  with certainty, we may simulate the same circuit with all coefficients evaluated mod  $p^e$ , and also reduce each of the coefficients  $h_t$  modulo  $p^e$ . If instead we are interested in whether a sequence of outcomes  $h_t$  arise with some probability (*e.g.* so that  $h_1$  occurs with probability  $p_1$ ,  $h_2$  occurs with probability  $p_{2|1}$  given that  $h_1$  occurred, etc.), we may express the probabilities in terms of a product of powers  $p^{-\gamma_t}$  for each prime divisor  $p$  of  $d$ , and simulate for each measurement  $1 \leq t \leq k$  whether or not the measurement outcome modulo  $p^e$  occurs with probability  $p^{-\gamma_t}$  by testing whether the measurement observable  $Z_{r_t}^{p^{e-\gamma_t}}$  stabilizes the state at measurement. As these problems may be contained in  $\text{coMod}_p\mathbf{L}$  for prime  $p$ , and characterize the *yes* instances for the same problems modulo  $d$ , these suffice to show:

**Theorem 9:** For any constant  $k \geq 1$ , for any stabilizer state given as input (described either as a standard basis state or via an initial stabilizer tableau), for any sequence  $h_1, \dots, h_k \in \mathbb{Z}_d$  of measurement outcomes, and for any sequence of conditional probabilities  $p_1, \dots, p_k$  of them occurring, the problem of determining whether the outcomes of the first  $k$  measurements are the outcomes  $h_j$  for  $1 \leq j \leq k$ , each with probability  $p_1 p_2 \dots p_j$ , is  $\text{coMod}_d\mathbf{L}$ -complete.

**N.B.** The issues described above relating to oracles do not arise if we are content to use a polynomial amount of workspace in the simulation. Simply using the tech-

niques of the preceding sections, we may easily simulate arbitrary stabilizer circuits with any number of measurements on standard basis states in polynomial time, by transforming stabilizer tableaus which are explicitly stored in the work space.

### C. Run time complexity

We conclude our considerations of the complexity of simulating stabilizer circuits with some remarks on more precise measures of complexity.

The computational complexity bounds of Sections V A and V B do not impose any bounds whatsoever on the run-time complexity, except that it is polynomial by virtue of  $\text{coMod}_d\text{L} \subseteq \text{NC}^2 \subseteq \text{P}$  [14]. In practice, the degree of this polynomial will be quite large, even for the non-deterministic logspace Turing machines [14] which are the usual model of computation used to define the class  $\text{coMod}_d\text{L}$ . Furthermore, using the techniques of Ref. [30], the degree of the run-time required to solve systems of linear equations modulo  $d$  will increase with the value of  $d$  — and with the number of measurements being simulated — according to the size of the prime-power factors of  $d$ . However, this is an expected trade-off in time for the savings in the work-space required by the algorithms outlined in Sections V A and V B. As  $\text{coMod}_d\text{L} \subseteq \text{NC}^2 \subseteq \text{DSPACE}(\log(n)^2)$ , the large running-time may be regarded as a consequence of simulating stabilizer circuits with a constant number of rounds of measurement, but of any size, with either Turing machines which require only  $O(\log(n)^2)$  space or polynomial-size boolean circuits of depth only  $O(\log(n)^2)$ . The techniques used to show containment in  $\text{coMod}_d\text{L}$  may be regarded as demonstrating upper bounds on the abstract computational power of stabilizer circuits (for any fixed number of measurement rounds) for any  $d \geq 2$ ; a more practical approach to simulating stabilizer circuits, on a computer architecture having a small number of processors but a substantial amount of memory, is simply to maintain an explicit record of stabilizer tableaus and measurement outcomes.

Apart from the results of Sections V A and V B, we may compare run-time complexity of the techniques of Sections III and IV to those of Ref. [11, Sec. III], for simulating stabilizer circuits on qubits with the more traditional “binary” representation on qubits (*i.e.* for the case  $d = 2$  alone). In this setting, we consider the complexity only of simulating a generator of the Clifford group (such as a Pauli operator or a gate corresponding to one of the operators in Eq. (15)), or of single-qubit  $Z$  measurements. It must be noted that despite the elimination of quadratic phase corrections in the simulation of Clifford operations, there is no improvement in the asymptotic complexity of simulating a single Clifford group operation compared to the results of Ref. [11]; it is  $O(n)$  in each case for a single gate acting on a tableau representing an  $n$ -qudit state (whether represented by a proper

tableau, or an extended tableau). Furthermore, the algorithm in Ref. [11] for simulating measurements in the case  $d = 2$  is more efficient than the algorithm presented in this article for simulating measurements, as the procedure presented in Section V B is essentially an extension of techniques of Ref. [1] to the case  $d \geq 2$ , for which Ref. [11] represents an improvement. Indeed, it seems likely that the techniques of Ref. [11, Sec. III] could be easily extended using the linear formalism of this article to achieve a complexity of  $O(n^2)$  for simulating  $Z$  measurements in any fixed *prime* dimension. However, as those techniques seem to rely on the fact that  $\mathbb{Z}_2$  (or  $\mathbb{Z}_d$  for prime  $d$ ) is a field, and in particular that the generating set for any stabilizer group has size at most  $n$ , it is not immediately clear how such techniques would extend even to the case of a prime power dimension. The improvement of the formalism of this article over that of Ref. [11] is not in terms of run-time complexity, but rather extending the space-bounded complexity theoretic results to arbitrary dimensions  $d \geq 2$ , and exploiting the reduction to linear algebra to do this more directly in the case of prime powers.

## VI. CONCLUSION

We have presented techniques to simulate unitary stabilizer circuits on qudits of any constant dimension  $d \geq 2$  using linear transformations, and simulate terminal measurements by solving systems of linear equations, using Weyl operators to represent Pauli operators. In particular: we demonstrate that the Clifford group can in each case be described effectively using only Pauli operators and a group representation of the symplectic group  $\text{Sp}_{2n}(\mathbb{Z}_D)$  over the integers modulo  $D$ , where  $D \in \{d, 2d\}$  is determined according to whether  $d$  is odd or even. We also present the first explicit treatment of the evolution of a state under measurement for composite dimension, and demonstrate how this may be achieved by linear transformations of an extended tableau. This leads to a simple, easy to use formalism for simulating stabilizer circuits on qudits of arbitrary dimension.

The motivation for the formalism of this article is not the actual run-time or circuit complexity, but rather a formalism for arbitrary dimension  $d \geq 2$  which is as uniform as possible, in which simulating individual operations is as simple as possible (in the sense that each operation involves fewer natural arithmetic operations). In doing so, we reduce the problem of simulation substantially to standard techniques of linear algebra, which is illustrated by the directness of the proof of Theorem 7 that simulating the measurement of a unitary stabilizer circuit is complete for the class  $\text{coMod}_d\text{L}$  for any  $d \geq 2$  (extending the computational complexity results of Aaronson and Gottesman [11]).

There remain open questions with respect to the efficient simulation of stabilizer circuits, which tools of the sort presented in this article may help address. We have

shown that stabilizer circuits on qudits of any fixed dimension, and any size, may be simulated in  $\text{NC}^2$  provided it has a fixed number of measurements, as this task is complete for  $\text{coMod}_d\text{L}$ . Is it possible to extend the number of measurements, for instance, to  $O(\log(n))$ , or (if we restrict the controlled-Clifford operations to controlled-Paulis) to  $O(n)$ ? Can similar results be obtained if we keep the number of measurements fixed, and perhaps even fix the size of the circuit, but allow the qudit dimension to be a prime power  $p^e$  (of a fixed prime  $p$ ) provided as input? Finally, what bounds can we obtain for simulating stabilizer circuits in a distributed classical computational model based on linear transformations, such as linear network coding [35]?

## Acknowledgements

A substantial part of this work was performed while I was working for the *Institut für Physik und Astronomie* at the Universität Potsdam, Potsdam, Germany, with support from the EU (QESSENCE, MINOS, COMPAS) and the EURYI scheme. The remainder was performed with support from the EC project QCS.

I would like to thank Earl Campbell, Matthias Ohliger, David Gross, Marcus Appleby, and the anonymous referees for helpful discussions and remarks on earlier drafts.

- 
- [1] D. Gottesman(1997), Ph.D thesis, quant-ph/9705052
  - [2] D. Gottesman, in *Group22: Proc. XXII International Colloquium on Group Theoretical Methods in Physics* (1998) pp. 32–43, arXiv:quant-ph/9807006
  - [3] R. Jozsa and A. Miyake, in *Proc. Roy. Soc. A*, Vol. 464 (2008) pp. 3089–3106, arXiv:0804.4050
  - [4] R. Jozsa, B. Kraus, A. Miyake, and J. Watrous, in *Proc. Roy. Soc. A*, Vol. 466 (2010) pp. 809–830
  - [5] M. van den Nest, *Quant. Info. & Comp.* **10**, 258 (2010)
  - [6] R. Raussendorf, D. E. Browne, and H. J. Briegel, *Phys. Rev. A* **68**, 022312 (2003), quant-ph/0301052
  - [7] A. M. Childs, D. W. Leung, and M. A. Nielsen, *Phys. Rev. A* **71**, 032318 (2005), quant-ph/0404132
  - [8] D. Gottesman, *Chaos, Solitons, and Fractals* **10**, 1749 (1999), quant-ph/9802007
  - [9] E. Hostens, J. Dehaene, and B. De Moor, *Phys. Rev. A* **71**, 042315 (2005), quant-ph/0408190
  - [10] P. W. Shor, in *Proc. 35th FOCS* (1994) pp. 124–134
  - [11] S. Aaronson and D. Gottesman, *Phys. Rev. A* **70**, 052328 (2004), quant-ph/0406196
  - [12] C. Damm, *Inf. Process. Lett.* **36**, 247 (1990)
  - [13] J. Dehaene and B. De Moor, *Phys. Rev. A* **68**, 042318 (2003), quant-ph/0304125
  - [14] G. Buntrock, C. Damm, U. Hertrampf, and C. Meinel, *Theory of Computing Systems* **25**, 223 (1992)
  - [15] V. Gheorghiu, S. Y. Looi, and R. B. Griffiths, *Phys. Rev. A* **81**, 032326 (2010), arXiv:0912.2017
  - [16] V. Gheorghiu, “Standard form of qudit stabilizer groups,” (2011), preprint, arXiv:1101.1519v1
  - [17] D. L. Zhou, B. Zeng, Z. Xu, and C. P. Sun, *Phys. Rev. A* **68**, 062303 (2003), quant-ph/0304054
  - [18] This differs from  $\tau = -\exp(i\pi/d)$  in Appleby [19]: these have similar features, but differ by a sign for  $d$  even. We choose  $\tau$  so that  $Y = i^\dagger Z^\dagger X^\dagger$  is a Weyl operator for  $d = 2$ .
  - [19] D. M. Appleby, *J. Math. Phys.* **46**, 052107 (2005)
  - [20] D. Gross and J. Eisert, *Quant. Info. & Comp.* **8**, 722 (2008), arXiv:0710.0651
  - [21] Note that the  $+1$ -eigenstates of an operator  $\tau^{-2\phi}W_v$  can also be described as  $\tau^{2\phi}$ -eigenstates of  $W_v$ . Phase coefficients may thus be used to denote powers of  $\tau^2$  as eigenvalues, describing a stabilized space as an intersection of the corresponding eigenspaces of the Weyl operators.
  - [22] Note that in the case of  $d$  even, the Weyl operators  $W_v$  for  $v \in \mathbb{Z}_D^{2n}$  are not linearly independent; then we must show that such a map  $\Phi$  is well-defined. However, by the discussion following Lemma 3,  $W_{Cv}$  cannot be expressed as a linear combination of other Weyl operators except if  $W_{Cv} = \pm W_{Cw}$  for some vector  $Cw \in \mathbb{Z}_D^{2n}$ , in which case the sign is given by  $(-1)^{[Cv, Cw]} = (-1)^{[v, w]}$  by Lemma 2. Then  $W_v = \pm W_w$  with the same sign, so that  $\Phi$  as described above is indeed well-defined.
  - [23] M. Grassl, M. Roetteler, and T. Beth, *Intl. J. Found. Comp. Sci.* **14**, 757 (2003), quant-ph/0211014
  - [24] In the case of  $M_a$ , we may represent  $a \in \mathbb{Z}_D^*$  by an integer  $0 < \alpha < D$  which is coprime to  $d$ ; then  $\alpha$  is also coprime to  $D$ , and the expression  $\alpha^{-1}$  represents an integer for which  $\alpha\alpha^{-1} \equiv 1 \pmod{D}$ . There are at most two such integers  $0 < \alpha < D$ ; it is easy to show that the operators  $M_a$ ,  $X^a$ , and  $Z^{a^{-1}}$  arising from them will be the same.
  - [25] In the construction of Ref. [9, Sec. IV], as in the formalism of this article, one- and two-qudit operations in many-qudit arrays are represented by applying a suitable choice of embedding of  $\text{Sp}_2(\mathbb{Z}_D)$  and  $\text{Sp}_4(\mathbb{Z}_D)$  into  $\text{Sp}_{2n}(\mathbb{Z}_D)$ , specifically one which respects the indexing of the qudits being acted on.
  - [26] Note that as we only use results of Hostens *et al.* [9] concerning generation of  $\text{Sp}_{2n}(\mathbb{Z}_D)$  which hold for arbitrary moduli  $D \geq 2$  and size  $2n > 0$ , the fact that our representation of stabilizer tableaux differs from theirs does not play any role in the proof.
  - [27] A. Kitaev, “Quantum measurements and the abelian stabilizer problem,” (1995), preprint, arXiv:quant-ph/9511026v1
  - [28] G. Nebe, E. M. Rains, and N. J. A. Sloane, *Designs, Codes, and Cryptography* **24**, 99 (2001)
  - [29] E. T. Campbell, H. Anwar, and D. E. Browne, “Magic state distillation in all prime dimensions using quantum reed-muller codes,” (2012), arXiv:1205.3104
  - [30] N. de Beaudrap, “On the complexity of solving linear congruences and computing nullspaces modulo a constant,” (2012), preprint, arXiv:1202.3949
  - [31] U. Hertrampf, S. Reith, and H. Vollmer, *Inf. Process. Lett.* **75**, 91 (August 2000)
  - [32] The class  $\text{coMod}_d\text{L}$  is usually defined as the class of decision problems for which there is a nondeterministic logspace Turing machine which accepts on a number of computational branches which is divisible by  $d$  if and only if the input is a *yes* instance. However, this pre-

cise definition is not particularly useful for our analysis. We will rely upon the characterization in terms of verifying coefficients of matrix products [14], which is a standard approach in the literature to showing relationships of problems to  $\text{coMod}_d\mathbf{L}$ .

- [33] Simulating networks made of reversible addition gates (that is,  $\Lambda X$  circuits) on tuples over  $\mathbb{Z}_d$  is a hard problem for  $\text{coMod}_d\mathbf{L}$ ; this may be shown by a reduction from matrix powering, using the standard reduction from matrix powering to matrix inversion described by Cook [36] and decomposing the upper-triangular matrices involved into elementary row operations, which is precisely how  $\Lambda X$  acts on standard basis states.
- [34] Note that no currently known techniques are known to simulate a tower of  $\text{coMod}_p\mathbf{L}$  oracles of unbounded depth, on a  $\text{coMod}_p\mathbf{L}$  machine; thus the distinction between  $k \in O(1)$ , and any number of measurements growing with the circuit size, is important.
- [35] R. Ahlswede, N. Cai, S.-Y. R. Li, and R. W. Yeung, IEEE Transactions on Information Theory **46**, 1204 (2000)
- [36] S. A. Cook, Information and Control, 2(1985)
- [37] Every non-zero vector in an actual vector space is fundamental, as  $\gcd(x, p) = 1$  for  $1 \leq x < p$  and  $p$  prime. This may be construed as precisely why stabilizer formalisms are easier to formulate in that case.

## Appendix A: Proper stabilizer tableaux and symplectic Clifford transformations

We now show that any generating set for a stabilizer group over  $\mathcal{H}_d^{\otimes n}$  has a proper stabilizer tableau, for  $d$  prime or odd. We also show how the same techniques apply to prove the “lifting” claim of Theorem 5.

### 1. Proper stabilizer tableaux for $d$ prime and $d$ odd

For  $d$  either prime or odd, we wish to show that any sequence  $S_1, \dots, S_\ell \in \mathcal{P}_d^{\otimes n}$  of commuting Pauli operators (each with order at most  $d$ ) may be represented by a sequence of vectors  $\bar{\mathbf{v}}_1, \dots, \bar{\mathbf{v}}_\ell \in \mathbb{Z}_d^{2n}$  and phases  $\varphi_1, \dots, \varphi_\ell \in \mathbb{Z}_D$  such that  $S_j = \tau^{-2\varphi_j} W_{\bar{\mathbf{v}}_j}$ , and for which  $[\bar{\mathbf{v}}_h, \bar{\mathbf{v}}_j] \equiv 0 \pmod{D}$  for all  $0 \leq h, j \leq \ell$ . This is in fact trivially true in the case of  $d$  odd: from the hypothesis that the operators  $S_j$  commute pair-wise, it follows that  $[\bar{\mathbf{v}}_h, \bar{\mathbf{v}}_j] \equiv 0 \pmod{D}$  by Lemma 1 for any Pauli vectors  $\varphi_j \oplus \bar{\mathbf{v}}_j$  representing the operators  $S_j$  as above. Thus, all stabilizer tableaux are proper for  $d$  odd.

It remains to prove the result for the binary case  $d = 2$ . More generally, for any even  $d$ , we may construct a proper tableau for the operators  $S_j$ , provided  $S_1^{m_1} S_2^{m_2} \dots S_\ell^{m_\ell} = \mathbb{1}$  only if each  $m_j$  is even. This holds, for example, for  $\{Z_1, Z_2, \dots, Z_n\}$  on  $n$  qudits, or any family of operators  $S_j = U Z_j U^\dagger$  obtained from them by conjugation by  $U \in \mathcal{C}_n(d)$ . We set  $\bar{\mathbf{v}}_1 = \mathbf{v}_1$ , and for each subsequent  $j > 1$ , we construct  $\bar{\mathbf{v}}_j = \bar{\mathbf{v}}_j + d\mathbf{x}_j$  for  $\mathbf{x}_j \in \mathbb{Z}_d^{2n}$  which satisfies

$$[\mathbf{v}_j, \bar{\mathbf{v}}_j] \equiv 0 \pmod{2d} \quad \text{and} \quad (\text{A1a})$$

$$[\bar{\mathbf{v}}_h, \bar{\mathbf{v}}_j] \equiv 0 \pmod{2d} \quad \text{for all } 1 \leq h < j. \quad (\text{A1b})$$

We may construct such a vector  $\bar{\mathbf{v}}_j$  as follows. The first constraint above ensures that  $W_{\bar{\mathbf{v}}_j} = W_{\mathbf{v}_j}$ . As  $[\mathbf{v}_j, \mathbf{v}_j] = 0$ , we may simplify it to obtain  $[\mathbf{v}_j, d\mathbf{x}_j] \equiv 0 \pmod{2d}$ , or equivalently

$$[\mathbf{v}_j, \mathbf{x}_j] \equiv 0 \pmod{2}. \quad (\text{A2a})$$

For the second constraint above, note that as  $[\mathbf{v}_h, \mathbf{v}_j]$  is a multiple of  $d$  for each  $1 \leq h < j$ , we have  $[\bar{\mathbf{v}}_h, \mathbf{v}_j] = db_{h,j}$  for some  $b_{h,j} \in \mathbb{Z}$ ; we may then expand this constraint to obtain

$$\begin{aligned} 0 &\equiv [\bar{\mathbf{v}}_h, \bar{\mathbf{v}}_j] \equiv [\bar{\mathbf{v}}_h, \mathbf{v}_j] + [\bar{\mathbf{v}}_h, d\mathbf{x}_j] \\ &\equiv db_{h,j} + d[\mathbf{v}_h, \mathbf{x}_j] + 2d(\frac{d}{2})[\mathbf{x}_h, \mathbf{x}_j] \pmod{2d}, \end{aligned} \quad (\text{A2b})$$

which we may further simplify to

$$[\mathbf{v}_h, \mathbf{x}_j] \equiv b_{h,j} \pmod{2}. \quad (\text{A2c})$$

Let  $\mathbf{b}_j = b_{1,j}\hat{\mathbf{e}}_1 + \dots + b_{j-1,j}\hat{\mathbf{e}}_{j-1}$  and  $W_j = [\mathbf{v}_1 \dots \mathbf{v}_j]$ . The constraints imposed by Eqs. (A2a) and (A2c) are then equivalent to

$$W_j^\top \sigma_{2n} \mathbf{x}_j \equiv \mathbf{b}_j \pmod{2}. \quad (\text{A3})$$

Note that equations of the form  $S_1^{m_1} \dots S_{j-1}^{m_{j-1}} S_j^{-1} = \lambda \mathbb{1}$  can only have solutions for  $\lambda = 1$  in stabilizer groups; and we have specifically ruled out the possibility that we can obtain such an expression for  $\mathbb{1}$  using an odd exponent for  $S_j$  in our hypotheses. By Lemma 2, it follows that the vectors  $\mathbf{v}_j$  are linearly independent modulo 2, in which case Eq. (A3) is a solvable system of linear equations over  $\mathbb{Z}_2$ , with potentially many satisfactory solutions. Selecting any one of them to fix a value of  $\bar{\mathbf{v}}_j$ , we then construct the next vector  $\bar{\mathbf{v}}_{j+1}$ , and so forth until we have obtained a sequence of Weyl vectors  $\bar{\mathbf{v}}_1, \dots, \bar{\mathbf{v}}_\ell$  forming a proper stabilizer tableau for the operators  $S_1, \dots, S_\ell$ .

As we note above, the above technique can be applied for arbitrary qudit dimension  $d$  as well for stabilizer tableaux whose Weyl blocks have independent columns. For  $d$  composite, not all tableaux have this property. In particular, there exist stabilizer groups on  $n$  qudits which have more than  $n$  independent commuting generators, whose corresponding Weyl blocks therefore cannot have independent columns modulo 2 or any other prime. (See the beginning of Section IV A for an example, and Section IV A 3 for a more general bound on the number of independent generators.)

### 2. Symplectic transformations performed by Clifford operations

We may apply similar techniques to the above to prove the “lifting” claim made in Theorem 5. Note that if  $W_{\mathbf{v}_j} = UW_{\bar{\mathbf{e}}_j}U^\dagger$  for  $1 \leq j \leq 2n$ , the operators  $W_{\mathbf{v}_j}$  will all have order  $d$ , and will be independent as well by virtue of the independence of the operators  $W_{\bar{\mathbf{e}}_j}$ . In particular, the vectors  $\mathbf{v}_j$  will be linearly independent modulo  $d$ .

We may then apply the same lifting technique as above, except that rather than the constraints of Eq. (A1), we impose the constraints

$$[\mathbf{v}_j, \bar{\mathbf{v}}_j] \equiv 0 \pmod{2d} \text{ and} \quad (\text{A4a})$$

$$[\bar{\mathbf{v}}_h, \bar{\mathbf{v}}_j] \equiv \delta_{h,n+j} - \delta_{j,n+h} \pmod{2d} \text{ for } h < j, \quad (\text{A4b})$$

where  $\delta_{a,b}$  is the Kronecker delta. These same congruences will already hold modulo  $d$  (rather than  $2d$ ) by the preservation of commutation relations from the conjugation by  $U$ . By constructing each  $\bar{\mathbf{v}}_j := \mathbf{v}_j + d\mathbf{x}_j$  as before, the same analysis may be applied to obtain constraints on each  $\mathbf{x}_j$  sufficient to obtain the necessary inner products modulo  $2d$  as well. The matrix  $\bar{C} = [\bar{\mathbf{v}}_1 \cdots \bar{\mathbf{v}}_{2n}]$  that we obtain as a result is symplectic modulo  $D$ .

## Appendix B: Supporting Lemmata concerning Weyl operators, stabilizer groups, and Pauli measurements

We now present additional technical properties of Weyl operators and stabilizer groups which generalize the known results for  $d$  prime, to characterize of the evolution of stabilizer states upon measurement. In particular, we show that this evolution is always uniformly random over a coset of the form  $\kappa + \eta\mathbb{Z}_d$  for some  $\kappa, \eta \in \mathbb{Z}_d$ . Much of this appendix describes results and techniques which are both simple and standard for the case  $d = 2$  (see *e.g.* Ref. [1]) and for  $d$  prime (Ref. [8]). However, such techniques do not seem to have been explicitly described for  $d$  composite (for which technical obstacles exist, due *e.g.* to non-trivial operators  $Z^a$  and  $X^b$  which commute despite acting on a common qudit).

We again adopt the convention described at the beginning of Section III D, that a measurement of a Pauli operator  $P$  (of order at most  $d$ ) stands for the measurement of some Hermitian operator  $H$  with spectral diameter less than  $2\pi$ , such that  $P = \exp(iH)$ , and that the outcome is some  $h \in \mathbb{Z}_d$  such that the result corresponds to the detection of a  $\tau^{2a}$ -eigenvector of  $P$ . We also suppose all measurements to be non-destructive, leaving a residual system which is in an eigenstate of the observable  $H$ , and thus of the unitary operator  $P$ .

### 1. Spectral properties of Weyl operators

The following simple results about Weyl operators are helpful to demonstrate how stabilizer groups transform under measurements in Sections B 2 and B 3, and may be of interest in the study of stabilizer codes over  $\mathbb{Z}_d$ .

As  $W_{\mathbf{v}}^d = \mathbb{1}$  for all  $\mathbf{v} \in \mathbb{Z}^{2n}$ , the eigenvalues of every Weyl operator are integer powers of  $\tau^2$ . For  $d$  composite, however, not all Weyl operators exhibit all possible powers of  $\tau^2$  as eigenvalues. (This is true for  $d$  prime as well, if one includes the Weyl operator  $W_{\mathbf{0}} = \mathbb{1}$ .) The eigenvalues that are exhibited by a Weyl operator  $W_{\mathbf{v}}$ ,

and their multiplicities, are governed in a simple way by the numerical relationships of the coefficients of  $\mathbf{v}$ .

**Definition IX:** For a vector  $\mathbf{v} \in \mathbb{Z}_D^m$ , the *harmonic number*  $\eta(\mathbf{v}) = \gcd(v_1, \dots, v_m, d)$  of  $\mathbf{v}$  is the largest positive integer  $\eta \leq d$  such that  $\mathbf{v} \in \eta\mathbb{Z}_D^m$ . We will say that  $\mathbf{v}$  is *fundamental* if  $\eta(\mathbf{v}) = 1$ .

Accounting for the harmonic number is necessary to bridge the gap with the case of  $d$  prime [37] to obtain constructions for all  $d \geq 2$ . Weyl operators  $W_{\mathbf{v}}$  with  $\mathbf{v}$  fundamental have the greatest ability to “distinguish” between different states; Weyl operators other than these have fewer eigenvalues, and each eigenvalue has higher multiplicity, so that their eigenspaces decompose as the sum of multiple eigenspaces of some other Weyl operator.

**Lemma 10:** For each Weyl operator  $W_{\mathbf{v}} \in \mathcal{P}_d^{\otimes n}$ , there exists a symplectic Clifford operator  $U \in \sigma\mathcal{C}_n(d)$  such that  $UW_{\mathbf{v}}U^\dagger = Z_j^{\eta(\mathbf{v})}$  for any  $1 \leq j \leq n$ .

**Proof:** For  $\mathbf{v} \in \mathbb{Z}^{2n}$  fundamental, using the decomposition *e.g.* of Ref. [9, Sec. IV], one may show that there is a symplectic operation  $C$  such that  $C\mathbf{v} = \hat{\mathbf{e}}_n$ . This construction consists essentially of using row-reductions on a stabilizer tableau to compute the greatest common divisor of the coefficients of  $\mathbf{v}$ ; these row-reductions may be performed by left-multiplication by symplectic transformations. The operations needed to perform the row-reduction may be obtained by solving for coefficients  $a_j$  such that  $a_1v_1 + \dots + a_{2n}v_{2n} = 1$ . By the construction described in the proof of Lemma 6, there then exists a symplectic Clifford  $U \in \sigma\mathcal{C}_n(d)$  such that  $UW_{\mathbf{v}}U^\dagger = Z_n$  acting only on the  $n^{\text{th}}$  qudit; we can then map this to any operator  $Z_j$  by swaps. If  $\mathbf{v} \in \mathbb{Z}^{2n}$  is not fundamental, let  $\mathbf{u} = \mathbf{v}/\eta(\mathbf{v})$ ; this vector is fundamental, so that there exists an operator  $U$  such that  $UW_{\mathbf{u}}U^\dagger = Z_j$ . Then  $UW_{\mathbf{v}}U^\dagger = UW_{\mathbf{u}}^{\eta(\mathbf{v})}U^\dagger = Z_j^{\eta(\mathbf{v})}$ .  $\square$

Note that the algorithm of Ref. [9, Sec. IV] yields the described unitary  $U$  in polynomial time, presented as a Clifford circuit of size  $O(n \log(d))$ .

**Lemma 11:** For any  $n > 0$  and  $\mathbf{v} \in \mathbb{Z}^{2n}$ , the eigenvalues of  $W_{\mathbf{v}}$  are all of the integer powers of  $e^{2\pi i \eta(\mathbf{v})/d}$ , each of which occurs with multiplicity  $\eta(\mathbf{v}) d^{n-1}$ .

**Proof:** By Lemma 10,  $W_{\mathbf{v}}$  has the same spectrum as  $Z_n^{\eta(\mathbf{v})}$ . Taking  $Z_n$  as an operator acting on  $\mathcal{H}_d^{\otimes n}$ , its spectrum consists of all of the integer powers of  $\tau^2$  with multiplicity  $d^{n-1}$  (that is, equal multiplicity). As  $\eta(\mathbf{v})$  divides  $d$ , we may show that the spectrum of  $Z_n^{\mathbf{v}}$  is all of the  $(d/\eta(\mathbf{v}))^{\text{th}}$  roots of unity also with equal multiplicity, which is to say  $\eta(\mathbf{v})d^{n-1}$ ; the same then holds for  $W_{\mathbf{v}}$ .  $\square$

**Corollary 11a:** For any  $\mathbf{v} \in \mathbb{Z}_D^{2n}$ , the Weyl operator  $W_{\mathbf{v}}$  has order  $d/\eta(\mathbf{v})$ . In particular, it has order  $d$  if and only if  $\mathbf{v}$  is fundamental.

## 2. Stabilizer groups of one-dimensional subspaces and commuting measurement observables

In this section, we prove the usual connection of Pauli observables which commute with every element of the stabilizer group with that measurement yielding a deterministic outcome, generalized to the setting of  $d \geq 2$  arbitrary. To do so, we prove a characterization (which is well-known for  $d$  prime) of those stabilizer groups which describe unique pure states: they are maximal stabilizer groups, in the sense that any Pauli subgroup which strictly contains such a group is either nonabelian, or contains operators without  $+1$  eigenvalues. (Proofs in the case of  $d$  prime typically make use of the fact that  $\mathbb{Z}_d^{2n}$  is a field, which we cannot do for  $d$  composite.)

**Lemma 12:** Let  $\mathcal{S} = \{S_1, \dots, S_\ell\}$  be a generating set for a stabilizer group  $G_{\mathcal{S}}$  on  $n$  qudits. The following are equivalent:

- (i)  $G_{\mathcal{S}}$  stabilizes a unique state;
- (ii)  $G_{\mathcal{S}}$  is a *maximal* stabilizer group;
- (iii)  $G_{\mathcal{S}}$  is a stabilizer group of *maximum size* (and has cardinality  $d^n$ ).

We note property (iii) above to emphasize the distinction from (ii), and for the sake of completeness. We will be interested primarily in certifying when a stabilizer group is inextendible, rather than when it has some particular cardinality.

**Proof:** Let  $\mathcal{S} \subset \mathcal{P}_d^{\otimes n}$  be an arbitrary stabilizer group. For each generator  $S_j \in \mathcal{S}$ , let

$$\Pi_{S_j} = \frac{1}{d} \sum_{p=0}^{d-1} S_j^p = \frac{1}{|S_j|} \sum_{p=0}^{|S_j|-1} S_j^p, \quad (\text{B1})$$

where  $|S_j|$  is the multiplicative order of  $S_j$ . It is easy to show that this operator projects onto the  $+1$ -eigenspace of  $S_j$ . Then  $\Pi_{\mathcal{S}} = \Pi_{S_1} \Pi_{S_2} \dots \Pi_{S_\ell}$  projects onto the joint  $+1$ -eigenspace of  $\mathcal{S}$ . By expanding each of the projectors  $\Pi_j$ , we may show that

$$\Pi_{\mathcal{S}} = \frac{1}{|G_{\mathcal{S}}|} \sum_{S \in G_{\mathcal{S}}} S, \quad (\text{B2})$$

as the terms in the sum run over all distinct combinations of powers  $S_1^{p_1} S_2^{p_2} \dots S_\ell^{p_\ell}$ , generating each element of  $G_{\mathcal{S}}$ . (As the group  $G_{\mathcal{S}}$  is the direct product of the cyclic groups generated by the operators  $S_j$ , it follows that  $|G_{\mathcal{S}}|$  is equal to the product of the orders  $|S_j|$ .)

It is easy to show that (i)  $\iff$  (iii): if  $\mathcal{S}$  stabilizes a unique state, it follows that  $\text{Tr}(\Pi_{\mathcal{S}}) = 1$ , so that

$$1 = \text{Tr}(\Pi_{\mathcal{S}}) = \frac{1}{|G_{\mathcal{S}}|} \sum_{S \in G_{\mathcal{S}}} \text{Tr}(S) = \frac{\text{Tr}(\mathbb{1})}{|G_{\mathcal{S}}|}, \quad (\text{B3})$$

where the final equality holds because  $\mathbb{1}$  itself is the only element of  $G_{\mathcal{S}}$  that has non-zero trace. Thus,  $|G_{\mathcal{S}}| =$

$\text{Tr}(\mathbb{1}) = d^n$ ; and this cardinality is at a maximum, as  $\text{Tr}(\Pi_{\mathcal{S}})$  must be an integer. The converse is similar.

It is also easy to show (i)  $\implies$  (ii). Suppose  $\mathcal{S}$  stabilizes a unique state  $|\psi\rangle$ , which is to say that  $\text{Tr}(\Pi_{\mathcal{S}}) = 1$ . Let  $P \in \mathcal{P}_d^{\otimes n}$  be a Pauli operator which commutes with all of  $\mathcal{S}$ . It is easy to show that  $\mathcal{S}$  also stabilizes  $P|\psi\rangle$ : by the uniqueness of  $|\psi\rangle$ , we therefore have  $P|\psi\rangle = \lambda|\psi\rangle$  for some phase  $\lambda$ . Then  $\lambda^{-1}P$  stabilizes  $|\psi\rangle$ , so that

$$\Pi_{\mathcal{S}} = \lambda^{-1} P \Pi_{\mathcal{S}} = \frac{\lambda^{-1}}{|G_{\mathcal{S}}|} \sum_{S \in G_{\mathcal{S}}} PS. \quad (\text{B4})$$

By hypothesis, we then have

$$\frac{\lambda^{-1}}{|G_{\mathcal{S}}|} \sum_{S \in G_{\mathcal{S}}} \text{Tr}(PS) = \text{Tr}(\Pi_{\mathcal{S}}) = 1. \quad (\text{B5})$$

As  $\text{Tr}(PS) \neq 0$  only if  $PS \propto \mathbb{1}$ , this implies that there exists an operator  $\tilde{S} \in G_{\mathcal{S}}$  such that  $\tilde{S} \propto P^{-1}$ . As any two such operators would be proportional to one another, and can only be distinct if one of them failed to stabilize  $|\psi\rangle$ , such an operator is unique. Similarly, as  $\tilde{S} \propto \lambda P^{-1}$  both stabilize  $|\psi\rangle$ , these are equal as well. Then either  $P \in G_{\mathcal{S}}$ , in the case that  $\lambda = 1$ ; or the group obtained by extending  $G_{\mathcal{S}}$  by  $P$  contains  $\lambda \mathbb{1}$  for  $\lambda \neq 1$ , and is therefore not a stabilizer group. Thus the uniqueness of the state  $|\psi\rangle$  entails that  $G_{\mathcal{S}}$  is maximal as a stabilizer group in  $\mathcal{P}_d^{\otimes n}$ . It remains to show that uniqueness of the stabilized state is a necessary condition for maximality as a stabilizer group.

Suppose instead that  $G_{\mathcal{S}}$  does not stabilize a unique state, and let  $|\psi_0\rangle, |\psi_1\rangle \in \text{img}(\Pi_{\mathcal{S}})$  be independent states stabilized by  $G_{\mathcal{S}}$ . Consider the operator

$$\Gamma = |\psi_1\rangle\langle\psi_0| - |\psi_0\rangle\langle\psi_1|. \quad (\text{B6})$$

As the Weyl operators span the set of operators on  $\mathcal{H}_d^{\otimes n}$  (by the corollary to Lemma 3, on page 2), there exists some operator  $W_{\mathbf{v}}$  such that  $\gamma := \text{Tr}(W_{\mathbf{v}}^\dagger \Gamma) \neq 0$ . By construction,  $\Gamma$  has trace zero; and as  $\Gamma S = \Gamma = S \Gamma$  for every element  $S \in G_{\mathcal{S}}$ , we have  $\text{Tr}(S^\dagger \Gamma) = 0$  for all  $S \in G_{\mathcal{S}}$  as well. Thus  $W_{\mathbf{v}}$  is not proportional to any element of  $G_{\mathcal{S}}$ . However, for any  $W_{\mathbf{s}} \propto S \in G_{\mathcal{S}}$ , we have

$$\begin{aligned} \gamma &= \text{Tr}(W_{\mathbf{v}}^\dagger \Gamma) = \text{Tr}(W_{\mathbf{v}} (W_{\mathbf{s}} \Gamma W_{\mathbf{s}}^\dagger)) \\ &= \text{Tr}(\tau^{2[\mathbf{v}, \mathbf{s}]} W_{\mathbf{v}} \Gamma) = \tau^{2[\mathbf{v}, \mathbf{s}]} \gamma, \end{aligned} \quad (\text{B7})$$

where the penultimate equality holds by Lemma 1. Then  $[\mathbf{v}, \mathbf{s}] \equiv 0 \pmod{d}$  for all such  $\mathbf{s}$ , so that  $S$  and  $W_{\mathbf{v}}$  commute. It follows that  $W_{\mathbf{v}}$  commutes with all of  $G_{\mathcal{S}}$ .

While  $W_{\mathbf{v}}$  is not proportional to any element of  $G_{\mathcal{S}}$ , there is a minimal integer  $1 \leq s \leq d$  such that  $W_{\mathbf{v}}^s$  is proportional to some  $P \in G_{\mathcal{S}}$ . Let  $\eta = \text{gcd}(v_1, \dots, v_{2n}, d)$ : by Lemma 11,  $W_{\mathbf{v}}^s = W_{\mathbf{s}\mathbf{v}}$  has eigenvalues consisting of integer powers of  $\tau^{2s\eta}$  with equal multiplicity. As  $P \propto W_{\mathbf{v}}^s$  has a non-trivial  $+1$ -eigenspace, the same is true for  $P$ . It follows that  $P = \tau^{2s\eta r} W_{\mathbf{v}}^s$  for some  $0 \leq r < d$ .

Define  $S_* := \tau^{2\eta r} W_{\mathbf{v}}$ , which by construction satisfies  $\text{Tr}(S_*^\dagger \Gamma) = \tau^{-2\eta r} \text{Tr}(W_{\mathbf{v}}^\dagger \Gamma) \neq 0$ , and each of whose integer powers are either **(a)** an element of  $G_S$  or **(b)** not proportional to any element of  $G_S$ . In particular, as  $W_{\mathbf{v}}$  has order  $d/\eta$  by construction, the only powers of  $S_*$  which are proportional to the identity are in fact equal to  $\mathbb{1}$ . Consider then the group  $\overline{G}$  obtained by extending  $G_S$  by  $S_*$ . This group is abelian, as  $S_* \propto W_{\mathbf{v}}$  commutes with all of  $G_S$ . Because the intersection of  $\langle S_* \rangle$  and  $G_S$  is the subgroup  $\langle S_*^s \rangle$  by construction, we can decompose  $\overline{G}$  into cosets of the form  $S_*^t G_S$  for  $0 \leq t < s$ . Define the operator

$$\Pi_{\overline{G}} = \frac{1}{|\overline{G}|} \sum_{S \in \overline{G}} S : \quad (\text{B8})$$

it is not difficult to show that  $\Pi_{\overline{G}}^2 = \Pi_{\overline{G}}$ , so that this is a projection. Furthermore, as  $S_*^0 \mathbb{1}$  is the unique element of  $\overline{G}$  proportional to the identity, we obtain

$$\text{Tr}(\Pi_{\overline{G}}) = \frac{1}{|\overline{G}|} \sum_{S \in \overline{G}} \text{Tr}(S) = \frac{\text{Tr}(\mathbb{1})}{|\overline{G}|} > 0, \quad (\text{B9})$$

which implies that there exists a non-zero element of  $|\Psi\rangle \in \text{img}(\Pi_{\overline{G}})$  which is a  $+1$ -eigenvector of each element of  $\overline{G}$ . Thus  $\overline{G}$  is a Pauli stabilizer group which strictly contains  $G_S$ , establishing  $(ii) \implies (i)$ .  $\square$

This result has an important consequence for Pauli measurements:

**Corollary 12a:** Let  $|\psi\rangle \in \mathcal{H}_d^{\otimes n}$  be the unique  $+1$ -eigenstate of a stabilizer group  $G_S \subset \mathcal{P}_d^{\otimes n}$ , and  $P \in \mathcal{P}_d^{\otimes n}$  an operator of order at most  $d$  which commutes with every operator in  $G_S$ . Then  $|\psi\rangle$  is undisturbed by measurements of  $P$ , and has a definite outcome  $h$  such that  $\tau^{-2h} P \in G_S$ .

**Proof:** By the preceding Lemma, there exists a scalar  $\lambda$  such that  $\lambda P \in G_S$ . Then  $|\psi\rangle$  is an eigenvector of  $P$  and is undisturbed by measurement. As  $P$  has order at most  $d$ , we have  $P = \tau^{-2\varphi} W_{\mathbf{p}}$  for some integer vector  $\mathbf{p} \in \mathbb{Z}^{2n}$ : its eigenvalues consist of integer powers of  $\tau^2$ . The result of a  $P$  measurement on  $|\psi\rangle$  must be the  $h \in \mathbb{Z}_d$  for which  $\tau^{-2h} P \in G_S$ .  $\square$

### 3. Measurement of observables which do not commute with all stabilizer generators

Consider a maximal stabilizer group  $G_S \subset \mathcal{P}_d^{\otimes n}$  generated by a set of operators  $\mathcal{S} = \{S_1, \dots, S_\ell\}$ , stabilizing a state  $|\psi\rangle$ . We consider the effect on  $|\psi\rangle$  of the measurement of an operator  $P \propto W_{\mathbf{p}}$  such that  $P^d = \mathbb{1}$ , but which does not commute with every  $S_j \in \mathcal{S}$ .

#### a. Reduction to the case of one generator not commuting with the measurement observable

As in the case of  $d$  prime, we may reduce to the case where at most one stabilizer generator fails to commute with the measurement observable by considering different generating sets of  $G_S$ . For arbitrary  $d \geq 2$ , we may do this as follows.

For each  $1 \leq j \leq \ell$ , consider coefficients  $0 \leq \phi_j < d$  (not all zero) such that  $PS_jP^\dagger = \tau^{2\phi_j} S_j$ . Note that the phases which are induced on Weyl operators  $W_{\mathbf{v}}$  by commutation with  $P$  depend on  $[\mathbf{p}, \mathbf{v}]$ , which is linear in  $\mathbf{v}$ : thus the phases induced by commutation with  $P$  on an arbitrary  $S' \in G_S$  by commutation with  $P$  is given by  $m_1\phi_1 + \dots + m_\ell\phi_\ell$ , where the integers  $m_j$  are exponents such that  $S' = S_1^{m_1} \dots S_\ell^{m_\ell}$ . Let  $\eta = \text{gcd}(\phi_1, \dots, \phi_\ell, d)$ : there exist integer vectors  $\mathbf{x} \in \mathbb{Z}^{\ell+1}$  such that

$$\eta = -z_{\ell+1}d + \sum_{j=1}^{\ell} z_j\phi_j. \quad (\text{B10})$$

From the above remarks, there then exists an element  $T = S_1^{z_1} \dots S_\ell^{z_\ell} \in G_S$  for which  $PTP^\dagger = \tau^{2\eta} T$ . As  $\eta$  divides each coefficient  $\phi_j$ , let  $\tilde{\varphi}_j = \phi_j/\eta$ ; we may then generate  $G_S$  by the operators  $\tilde{\mathcal{S}} = \{\tilde{S}_0, \tilde{S}_1, \dots, \tilde{S}_\ell\}$ , setting  $\tilde{S}_0 := T$  and  $\tilde{S}_j := S_j T^{-\tilde{\varphi}_j}$  for  $1 \leq j \leq \ell$ .

#### b. The subgroup of stabilizers commuting with the measurement

In the above construction, each generator  $\tilde{S}_j$  commutes with  $P$  for  $1 \leq j \leq \ell$ . In the case that  $d$  is prime, they also generate the subgroup of  $G_S$  which commutes with the observable  $P$ . However, this does not hold for arbitrary  $d$ . For example, consider a  $Z_b$  measurement performed on a state  $|\psi\rangle_{a,b}$  of a system of two qudits  $a$  and  $b$ , where  $d = d_1 d_2$  (for  $d_1, d_2 > 1$ ) and where  $|\psi\rangle$  is stabilized by

$$|\psi\rangle_{a,b} = \Lambda X_{a,b}^{d_1} F_a |0\rangle_a |0\rangle_b. \quad (\text{B11})$$

This state is stabilized by  $\mathcal{S} = \{Z_a^{-d_1} Z_b, X_a X_b^{d_1}\}$ , as one may show by applying the transformations of Eq. (16) to the operators  $\{Z_b, Z_a^\dagger\}$  stabilizing the state  $|0\rangle_a |0\rangle_b$ . Let  $S_1 = Z_a^{-d_1} Z_b$  and  $S_2 = X_a X_b^{d_1}$ . Of the elements of  $\mathcal{S}$ , only  $S_2$  fails to commute with  $Z_b$ ; and we obtain  $\phi_1 = 0$ ,  $\phi_2 = d_1$ . We may set  $z_1 = 0$  and  $z_2 = 1$  to obtain  $\eta = d_1$ , and from this define

$$\begin{aligned} \tilde{S}_0 &= T = S_1^0 S_2^1 = X_a X_b^{d_1}, \\ \tilde{S}_1 &= S_1 T^0 = Z_a^{-d_1} Z_b, \\ \tilde{S}_2 &= S_2 T^{-1} = \mathbb{1}. \end{aligned} \quad (\text{B12})$$

Note that  $\{\tilde{S}_1, \tilde{S}_2\}$  alone fails to generate the operator  $X_a^{d_2} = S_2^{d_2} \in G_S$ , which commutes with  $P$ .



In the general case, we may characterize the subgroup of  $G_S$  which commutes with  $P$  as follows. Consider an arbitrary operator  $S' = \tilde{S}_0^{m_0} \tilde{S}_1^{m_1} \dots \tilde{S}_\ell^{m_\ell} \in G_S$  which commutes with  $P$ . As  $\tilde{S}_j^{m_j}$  commutes with  $P$  for each  $1 \leq j \leq \ell$ ,  $\tilde{S}_0^{m_0}$  must also commute with  $P$ , so that

$$\tilde{S}_0^{m_0} = P \tilde{S}_0^{m_0} P^\dagger = \tau^{2\eta m_0} \tilde{S}_0^{m_0}. \quad (\text{B13})$$

Then  $m_0$  is a multiple of  $d/\eta$ , so that the operators  $\mathcal{S}_C = \{\tilde{S}_0^{d/\eta}, \tilde{S}_1, \tilde{S}_2, \dots, \tilde{S}_\ell\}$  generate the subgroup of  $G_S$  commuting with  $P$ . (In the familiar case of  $d$  prime, we necessarily have  $\eta = 1$ , so that  $\tilde{S}_0^{d/\eta} = \mathbb{1}$  may be excluded as a generator; we then recover the result that  $\tilde{S}_1, \dots, \tilde{S}_\ell$  generate the commuting subgroup for  $d$  prime.)

*c. Characterization of the post-measurement state and distribution of outcomes*

Following the above analysis, suppose that we have a generating set  $\mathcal{S} = \{S_0, S_1, \dots, S_\ell\}$  in which only  $S_0$  fails to commute with  $P$ ; specifically, we may suppose  $P S_0 P^\dagger = \tau^{2\eta} S_0$  for some  $\eta$  a divisor of  $d$ . From the preceding section,  $\mathcal{S}_C = \{S_0^{d/\eta}, S_1, S_2, \dots, S_\ell\}$  generates the subgroup of  $G_S$  which commutes with  $P$ . The operators of  $\mathcal{S}_C$  also stabilize the post-measurement state: if we let

$$\Pi_h = \frac{1}{d} \sum_{j=1}^d (\tau^{-2h} P)^j \quad (\text{B14})$$

be the projector onto the  $\tau^{2h}$ -eigenspace of  $P$ , we have

$$S \Pi_h |\psi\rangle = \Pi_h S |\psi\rangle = \Pi_h |\psi\rangle \quad (\text{B15})$$

for any  $S \in G_{\mathcal{S}_C}$ . The post-measurement state is naturally also stabilized by  $R := \tau^{-2h} P = \tau^{-2u} W_{\mathbf{p}}$ , where  $h$  is the actual measurement outcome.

To consider the distribution of possible values of  $h \in \mathbb{Z}_d$ , consider a Weyl operator  $W_{\mathbf{p}} \propto P$ , and let  $u \in \mathbb{Z}_d$  be such that  $R = \tau^{-2u} W_{\mathbf{p}}$ . By hypothesis, we have  $W_{\mathbf{p}} S_0 W_{\mathbf{p}}^\dagger = \tau^{2\eta} S_0$ , with  $W_{\mathbf{p}} S_j W_{\mathbf{p}}^\dagger = S_j$  for all  $1 \leq j \leq \ell$ . Let  $s = d/\eta$ ; just as  $S_0^s$  is the smallest power of  $S_0$  which commutes with  $P \propto W_{\mathbf{p}}$ , we may show that

$$S_0 W_{\mathbf{p}}^s S_0^\dagger = (\tau^{-2d} W_{\mathbf{p}})^s = W_{\mathbf{p}}^s; \quad (\text{B16})$$

it follows that  $W_{\mathbf{p}}^s$  commutes with all elements of  $\mathcal{S}$ , and so is proportional to an element of  $G_S$  by Lemma 12.

Specifically, it is proportional to an element of  $G_{\mathcal{S}_C}$ , as  $W_{\mathbf{p}}^s$  commutes with  $P$ . The post-measurement state is then stabilized both by  $\tau^{-2u} W_{\mathbf{p}}$  and by  $W_{\mathbf{p}}^s$ . Thus the operator  $(\tau^{-2u} W_{\mathbf{p}})^s W_{\mathbf{p}}^{-s} = \tau^{-2su} \mathbb{1}$  stabilizes the post-measurement state, which implies that  $su \equiv 0 \pmod{d}$ , i.e. that  $u$  is a multiple of  $d/s = \eta$ . The result of measuring  $P$  then satisfies  $h \in \kappa + \eta \mathbb{Z}_d$ , where  $P = \tau^{-2\kappa} W_{\mathbf{p}}$ .

The distribution of measurement outcomes within the coset  $\kappa + \eta \mathbb{Z}_d$ , and the relationships between them, straightforwardly generalize the standard results for  $d$  prime. Let  $\Pi_h$  again be the projection onto the  $\tau^{2h}$ -eigenspace of  $P$  as given in Eq. (B14): then

$$\begin{aligned} S_0 \Pi_h &= \frac{1}{d} \sum_{j=1}^d S_0 (\tau^{-2h} P)^j \\ &= \frac{1}{d} \sum_{j=1}^d (\tau^{-2h-2\eta} P)^j S_0 = \Pi_{h+\eta} S_0. \end{aligned} \quad (\text{B17})$$

It follows then that  $S_0 \Pi_h |\psi\rangle = \Pi_{h+\eta} |\psi\rangle$ . By repeated application of  $S_0$ , we can iterate through all the elements of  $\kappa + \eta \mathbb{Z}_d$ , from which it follows that (a) all measurement outcomes in  $\kappa + \eta \mathbb{Z}_d$  are equally likely, as the vectors  $\Pi_{\kappa+\eta z} |\psi\rangle$  have the same norm; and (b) the post-measurement state for the outcome  $h$  can be transformed to that for  $h + \eta z$  by performing the operation  $S_0^z$ . Thus the “eliminated” stabilizer generator  $S_0$  of the pre-measurement state becomes a unitary byproduct operator (in the sense of Ref. [6]) which relates the possible post-measurement states; and the measurement outcome  $h$  is uniformly distributed over the coset  $\kappa + \eta \mathbb{Z}_d$ , where  $\tau^{2\kappa} P$  is a Weyl operator.

Note that the above analysis can accommodate the case of a deterministic measurement outcome, if we do not assume at the outset that  $P$  does not commute with all of  $G_S$ . If  $W_{\mathbf{p}}$  commutes with all elements of  $\mathcal{S}$ , it follows that  $\eta = d$ , in which case the solution set to Eq. (25) is a singleton modulo  $d$ : the distribution of outcomes is then the “uniform distribution” on that singleton set, i.e. a delta distribution on the sole solution  $h$ .

As we have remarked previously, the familiar case for  $d$  prime corresponds to  $\eta = 1$  provided that  $P$  does not commute with all elements of  $G_S$ . Then Eq. (25) trivializes, imposing no constraints on the value of  $h$ . The outcome is then uniformly distributed over all  $h \in \mathbb{Z}_d$ . The generalization for  $d$  composite is that the measurement outcome may in principle be uniformly distributed over a coset of any additive subgroup of  $\mathbb{Z}_d$ , and not just on some singleton set or on  $\mathbb{Z}_d$  itself.